Sayısal Takograf Sistemi
Türkiye Ulusal Otoritesi (TR-A) Politikası

Ver. 1.0

Revizyon 23.07.2010

DİZİN

1 Giriş

Bu doküman Sayısal Takograf Sistemi için Türkiye Ulusal Otoritesi (TR-A) Politikası'dır. Bu Politika aşağıda yer alan yayınlar ile uyumludur:

- COUNCIL REGULATION (EC) No 2135/98 of 24 September 1998 amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/84 and (EEC) No 3821/85
- European Agreement Concerning the Work of Crews of Vehicles Engaged in International Road Transport (AETR) concluded at Geneva on 1 July 1970
- Memorandum of Understanding between the European Commission services and UNECE, January 2009
- Commission Regulation (EC) No 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport
- the "Guideline and Template National Certification Authority policy" – Version 1.0
- the "Common Security Guidelines" – Version 1.0
- Digital Tachograph System European Root Policy, Version 2.1; European Commission Joint Research Center Publication 53429; 28th July 2009; published at http://dtc.ec.europa.eu.

1.1 Sorumlu Organizasyon

Bu Politikanın uygulama sorumlusu, Sözleşme Otoritesi (**CPA**) olan T.C. Ulaştırma Bakanlığı Kara Ulaştırma Genel Müdürlüğü'dür (KUGM) ve bundan sonra **TR-A**[1] olarak ifade edilecektir.

T.C. Ulaştırma Bakanlığı
Kara Ulaştırması Genel Müdürlüğü (KUGM)
Hakkı Turayliç Cad. No: 5
Emek/Ankara
TÜRKİYE

Görevlendirilmiş Kart Verme Otoritesi (**CIA**) "Türkiye Odalar ve Borsalar Birliği" (TOBB)'dir ve bundan sonra **TR-CIA**[2] olarak ifade edilecektir.

Görevlendirilmiş Sertifika Üretim Otoritesi (**CA**) "Türkiye Odalar ve Borsalar Birliği" (TOBB)'dir ve bundan sonra **TR-CA**[3] olarak ifade edilecektir.

Görevlendirilmiş Kart Kişiselleştirme Organizasyonu (**CP**) "Türkiye Odalar ve Borsalar Birliği" (TOBB)'dir ve bundan sonra **TR-CP**[4] olarak ifade edilecektir.

"Türkiye Odalar ve Borsalar Birliği" (TOBB) TR-CA veya TR-CP olarak süreçlerinden bir kısmını Hizmet Kuruluşu olarak adlandırılan alt yükleniciler aracılığıyla gerçekleştirebilir. Hizmet Kuruluşlarının kullanılması, hiçbir takdirde TR-CA ve TR-CP'nin genel sorumluluğunu azaltmaz.

TR-CA ve TR-CP için Görevlendirilmiş Hizmet Kuruluşu:

TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
Hollanda Cad. 696.Sok. No:7 Yıldız Çankaya ANKARA 06550 TÜRKİYE
Telefon: (312) 439 10 00
Faks: (312) 439 10 01
Web: www.turktrust.com.tr

[1] **TR-A** – Türkiye Ulusal Otoritesi
[2] **TR-CIA** – Türkiye Kart Verme Otoritesi
[3] **TR-CA** – Türkiye Sertifika Üretim Otoritesi
[4] **TR-CP** – Türkiye Kart Kişiselleştirme Organizasyonu

1.2 Onay

Bu Politika, Sayısal Takograf Kök Sertifikası Üretim Otoritesi (Digital Tachograph Root Certification Authority) tarafından … …….… 2010 tarihinde Avrupa Komisyonu (European Commission) için onaylanmıştır.

Digital Tachograph Root Certification Authority
Traceability and Vulnerability Assessment Unit
European Commission
Joint Research Centre, Ispra Establishment (TP.360)
Via E. Fermi, 1
I-21020 Ispra (VA)

1.3 Erişim ve İletişim bilgileri

Bu Politikaya T.C. Ulaştırma Bakanlığı KUGM'ye ait olan http://www.kugm.gov.tr web sitesinden ulaşılabilir.
Bu Politika ile ilgili sorular aşağıdaki adrese iletilmelidir:

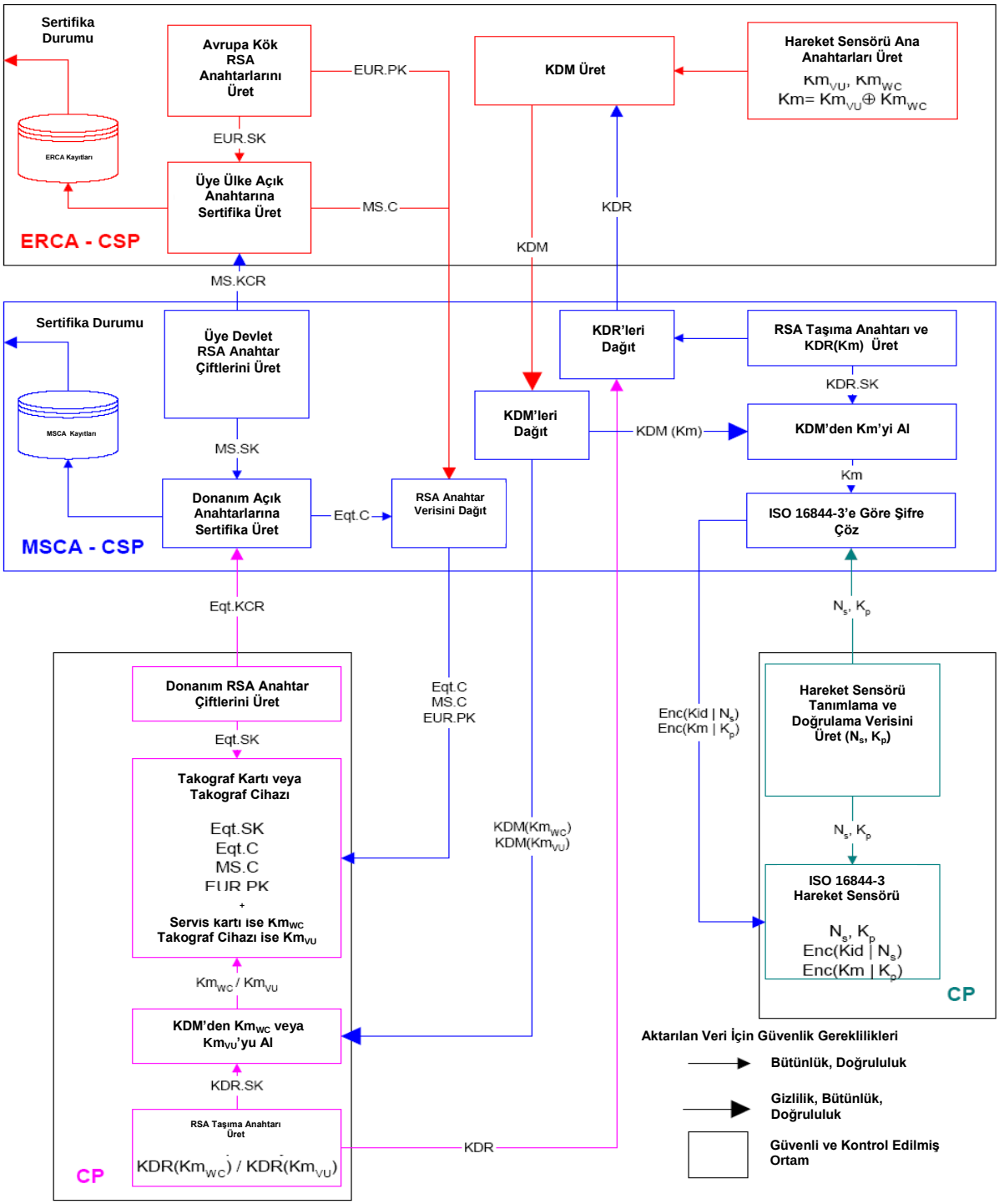
T.C. Ulaştırma Bakanlığı
Kara Ulaştırma Genel Müdürlüğü (KUGM)
Hakkı Turayliç Cad. No: 5
Emek/Ankara
TÜRKİYE

2 Kapsam ve Uygulanabilirlik

[r1] Bu Politika sadece Takograf sistemi için geçerlidir.

[r2] TR-CA tarafından üretilen anahtarlar ve sertifikalar sadece Takograf sisteminde kullanılır.

[r3] Sistem tarafından üretilen Kartlar sadece Takograf sisteminde kullanılır.
Takograf sistemi içerisinde bu Politikanın kapsamı aşağıdaki şekilde gösterilmiştir.



3 Genel Hükümler

Bu bölüm, TR-A, TR-CIA, TR-CA, TR-CP, Hizmet Kuruluşları ve kullanıcıların ayrı ayrı yükümlülükleri ile ilgili hükümler, kanun ve uyuşmazlıkların çözümlenmesi ile ilgili diğer konuları içerir.

3.1 Yükümlülükler

Bu bölüm aşağıdaki rollerin ayrı ayrı yükümlülükleri ile ilgili hükümleri içerir:

- TR-A ve TR-CIA
- TR-CA ve Hizmet Kuruluşu (eğer varsa)
- TR-CP ve Hizmet Kuruluşu (eğer varsa)
- Kullanıcılar (Kart sahipleri, VU üreticileri ve Hareket Sensörü üreticileri)

3.1.1 TR-A ve TR-CIA'nın Yükümlülükleri

Bu Politikaya göre TR-A ve TR-CIA'nın yükümlülükleri aşağıdaki gibidir.

[r4] TR-A:

a) Bu Politikanın devamlılığını sağlar.
b) TR-CA ve TR-CP görevlendirir.
c) Görevlendirilmiş TR-CA, TR-CP ve Hizmet Kuruluş'larını denetler.
d) TR-CA/TR-CP Uygulama Esasları dokümanını onaylar.
e) Görevlendirilmiş tarafları bu Politika hakkında bilgilendirir.
f) Bu Politikanın Komisyon tarafından onaylanmasını sağlar.

[r5] TR-CIA:

a) Başvuru sürecinde alınan doğru ve uygun kullanıcı bilgilerinin TR-CA ve TR-CP'ye girdi olmasını sağlar.
b) Kullanıcıları (Kart sahipleri, Takograf Cihazı üreticileri ve Hareket Sensörü üreticileri) sistemin kullanımı ile ilgili Politikada belirtilen gereklilikler hakkında bilgilendirir.

3.1.2 TR-CA'nın Yükümlülükleri

[r6] Görevlendirilmiş TR-CA:

a) Bu Politika uyarınca faaliyet gösterir.
b) Bu Politikayı referans alan ve TR-A tarafından onaylanan bir TR-CA Uygulama Esasları dokümanı yayımlar.
c) Bu Politikada belirtilen gerekliliklere uygun faaliyet göstermek ve özellikle hatalı işleyişten dolayı ortaya çıkabilecek zararların riskini karşılamak için yeterli organizasyon ve finansal kaynağı sağlar.

[r7] TR-CA, kendisi için bu Politikada belirlenmiş tüm gereklilikleri sağladığını garanti eder.

[r8] TR-CA faaliyetleri Hizmet Kuruluşları olarak adlandırılan alt yükleniciler tarafından gerçekleştiriliyor olsa bile, TR-CA'nın kendisi için bu Politikada belirlenmiş tüm prosedürlere uyma sorumluluğu vardır. TR-CA, Hizmet Kuruluşu'nun tüm hizmetlerini Uygulama Esasları'na (PS) ve bu Politikaya uygun sunmasını sağlamak ile sorumludur.

3.1.3 TR-CP'nin Yükümlülükleri

[r9] Görevlendirilmiş TR-CP (kart kişiselleştirme organizasyonu):

a) Bu Politika uyarınca faaliyet gösterir.
b) Bu Politikayı referans alan ve TR-A tarafından onaylanan bir TR-CP Uygulama Esasları dokümanı yayımlar.
c) Bu Politikada belirtilen gerekliliklere uygun faaliyet göstermek ve özellikle hatalı işleyişten dolayı ortaya çıkabilecek zararların riskini karşılamak için yeterli organizasyon ve finansal kaynağı sağlar.

[r10] TR-CP, kendisi için bu Politikada belirlenmiş tüm gereklilikleri sağladığını garanti eder.

[r11] TR-CP faaliyetleri Hizmet Kuruluşları olarak adlandırılan alt yükleniciler tarafından gerçekleştiriliyor olsa bile, TR-CP'nin kendisi için bu Politikada belirlenmiş tüm prosedürlere uyma sorumluluğu vardır.

3.1.4 Hizmet Kuruluşu Yükümlülükleri

[r12] Hizmet Kuruluşlarının, TR-CA veya TR-CP ve kullanıcılara karşı sözleşmeli anlaşmalara göre yükümlülükleri vardır.

3.1.5 Kart Sahibinin Yükümlülükleri

[r13] TR-CIA, anlaşmaya göre (bakınız 5.1.2) kullanıcının (veya kullanıcının organizasyonunun) aşağıdaki yükümlülüklere uymasını zorunlu kılar:

a) Bu politikanın gerekliliklerine ve özellikle kayıt süreci ile ilgili olan şartlara göre doğru ve eksiksiz bilginin TR-CIA'ya verilmesi;
b) Anahtar ve sertifikaların sadece Takograf Sistemi'nde kullanılması;
c) Kartın sadece Takograf Sistemi'nde kullanılması;
d) Donanım gizli anahtarı ve kartın yetkisiz kişilerce kullanılmasını önlemek için gerekli tedbirlerin alınması;
e) Kullanıcı sadece kendi anahtarlarını, sertifikasını ve kartını kullanabilir (AETR 11.4.a);
f) Kullanıcının sadece bir adet geçerli sürücü kartı olabilir (AETR 11.4.a);
g) Kullanıcı ancak çok özel şartlar altında makul bir mazeretle hem servis hem yedek şirket kartına (AETR Ek 1B VI: 1) veya hem servis hem sürücü kartına veya birkaç tane servis kartına sahip olabilir;
h) Kullanıcı hasarlı veya süresi dolmuş kartı kullanamaz (AETR 11.4.a);
i) Kullanıcı, sertifika içinde belirtilmiş geçerlilik süresinin bitimine kadar aşağıdaki durumların her hangi birinin meydana gelmesi durumunda, TR-CIA'yı her hangi bir gecikme olmadan bilgilendirir:
   - Donanım gizli anahtarı veya kart kayıp olur, çalınır veya potansiyel bir tehlike ile karşı karşıya kalırsa; (AETR 12.1)
   - Sertifika içeriği hatalı hale gelirse.

3.1.6 Takograf Cihazı Üreticilerinin Yükümlülükleri (kişiselleştirme organizasyonu olarak görev alan)

Şu an veya yakın gelecekte Türkiye'de uygulanabilir değildir.

3.1.7 Hareket Sensörü Üreticilerinin Yükümlülükleri (kişiselleştirme organizasyonu olarak görev alan)

Şu an veya yakın gelecekte Türkiye'de uygulanabilir değildir.

3.2 Sorumluluk

TR-CA ve TR-CP sorumluluğu sadece TR-A ve TR-CIA'dır, son kullanıcılara karşı sorumluluğu yoktur. Son kullanıcılara karşı sorumluluk sahibi TR-A/TR-CIA'dır.

[r16] Takograf kartları, anahtarları ve sertifikaları sadece Takograf sisteminde kullanılır, her hangi bir başka sertifikanın Takograf kartlarında bulunması, bu Politikanın ihlali anlamına gelmektedir ve bu durumda TR-A, TR-CIA, TR-CA veya TR-CP'den hiç biri herhangi bir sorumluluk taşımamaktadır.

3.2.1 TR-A ve TR-CIA'nın Kullanıcılara ve 3. Kişilere Karşı Sorumluluğu

[r17] TR-A ve TR-CIA sadece ihmalkârlık yaptığı takdirde yükümlülüklerini yerine getirmemekten dolayı oluşan zararlardan sorumludur. Eğer TR-A ve TR-CIA, bu Politika ve herhangi bir ilgili kanun/ yasal düzenlemeler uyarınca hareket etmişse, bu durum ihmalkârlık olarak nitelendirilemez.

3.2.2 TR-CA ve TR-CP'nin TR-A ve TR-CIA'ya Karşı Sorumluluğu

[r18] TR-CP ve TR-CA sadece ihmalkârlık yaptığı takdirde yükümlülüklerini yerine getirmemekten dolayı oluşan zararlardan sorumludur. Eğer organizasyon, bu Politika ve ilgili UE ile herhangi bir ilgili kanun/yasal düzenlemeler uyarınca hareket etmişse, bu durum ihmalkârlık olarak nitelendirilmez.

3.3 Yasal Düzenleme

3.3.1 Uygulanan Kanun

Sayısal Takograf Sistemi'nin geçekleştirilmesi ve yürütülmesi ile ilgili olan tüm konularda, yürürlükte olan Türkiye Cumhuriyeti Kanunları'na göre karar verilir.

3.4 Gizlilik

Gizlilik, Avrupa Birliği Direktifi 95/46/EC ve kişisel bilgilerin korunması ve taşınması hakkında 01.06.2005 tarihinde yürürlüğe giren 5237 Sayılı Türk Ceza Kanunu uyarınca sağlanmaktadır.

3.4.1 Gizli Tutulması Gereken Bilgiler

[r19] TR-CA, TR-CP veya Hizmet Kuruluşu tarafından tutulan, üretilmiş kart üzerinde görülmeyen veya sertifikalarda bulunmayan herhangi bir kişisel veya kurumsal bilgi gizli olarak nitelendirilmiştir. Bu bilgilerin gizliliği Kanun gerektirmedikçe, kullanıcının veya kullanıcının işvereninin veya temsilcisinin (uygulanabilir olduğunda) izni olmadan kaldırılmaz.

[r20] Bu Politika kapsamında TR-CA/TR-CP süreçlerinde kullanılan tüm özel ve gizli anahtarlar gizli olarak tutulmaktadır.

[r23] Kanunun gerektirmesi dışında, denetim logları ve kayıtları bir bütün olarak herkesin erişimine açık olarak tutulmamaktadır.

3.4.2 Gizli Olmayan Bilgiler

[r24] Sertifikalar gizli değildir.

[r25] Yasal düzenlemeler veya özel anlaşmalarca aksi belirtilmedikçe, kart üzerinde görülen veya sertifikalarda bulunan kimlik bilgileri, diğer kişisel veya kurumsal bilgiler gizli olarak nitelendirilmemişlerdir.

4 Uygulama Esasları (UE)

[r26] TR-CA ve TR-CP, bu Politika'da belirlenen bütün gereklilikleri referans alan, uygulamalar ve prosedürlere ait esasları içeren Uygulama Esasları'na (UE) göre faaliyet gösterir. TR-A UE'yi onaylar. Özellikle:

a) UE, TR-CA ve CP'ye hizmet sağlayan tüm dış organizasyonların, uygulanabilir politikaları ve uygulamaları dâhil yükümlülüklerini belirler.
b) Uygulama Esasları, TR-A, Takograf Sistemi kullanıcıları ve 3. kişiler'in (örn. denetim kurumları) erişimine açıktır. Ancak TR-CA/TR-CP genellikle uygulamalarının tüm detaylarının herkesçe erişilebilir olmasını sağlamak zorunda değildir.
c) TR-CA/TR-CP'nin yönetimi, UE'nin tam olarak uygulanmasını sağlamak ile yükümlüdür.
d) TR-CA/TR-CP, UE için gözden geçirme süreci belirler.
e) TR-CA/TR-CP, kendi UE'sinde düzeltme yapmak için bilgilendirmede bulunur ve onayı takiben güncellenmiş UE'yi en kısa sürede erişilebilir duruma getirir. Küçük düzeltmeler içeren revizyonlar TR-A onayı olmadan yayımlanabilir.

5 Donanım Yönetimi

Takograf Sistemi'ndeki donanımlar aşağıda verilmiştir:

- Takograf kartları
- Takograf cihazları
- Hareket sensörleri

Donanımlar aşağıda verilmiş kuruluşlar tarafından kullanılır ve yönetilir:

- TR-CIA (kayıt, yenileme, vb.)
- TR-CA (sertifikalar, anahtarlar)
- TR-CP (görsel ve elektronik kişiselleştirme, dağıtım, iptal)
- Takograf Cihazı üreticileri ve Hareket Sensörü üreticileri

TR-A tarafından gerçekleştirilen faaliyetler:

- Kalite kontrol (tip onayı)

TR-CIA tarafından gerçekleştirilen faaliyetler:

- Kart Başvurusu
- Başvuru onaylama ve kayıt
- Donanım kayıtı ve veri depolama (DB)

TR-CA ve TR-CP tarafından gerçekleştirilen faaliyetler:

- Kalite kontrol (örnek testleri)
- Anahtar üretimi
- Kart kişiselleştirme
- Dağıtım

Takograf üreticilerinin gerçekleştirdiği faaliyetler bu Politikanın kapsamı dışındadır.
Hareket sensörü üreticilerinin gerçekleştirdiği faaliyetler bu Politikanın kapsamı dışındadır.

5.1 Takograf Kartları

5.1.1 Kalite Kontrol – TR-CA/TR-CP Faaliyeti

[r27] TR-CA/TR-CP, Takograf Sistemi'nde sadece AETR'ye göre tip onayı almış kartların kişiselleştirme işleminin yapılmasını sağlar. Ayrıca bakınız 5.1.7.5.

5.1.2 Kart Başvurusu – TR-CIA Faaliyeti

[r28] TR-CIA, kartların kullanımında uyulması gereken şartlar ve koşullar hakkında kullanıcıları bilgilendirir. Bu bilgilendirmenin en az Türkçe ve İngilizce dillerinde erişilebilir olmasını sağlar.

[r29] Kullanıcı kart başvurusu yaparak ve kartı teslim alarak, tüm şartları ve koşulları kabul etmiş olur.

5.1.2.1 Kullanıcı Uygulaması

[r30] Kart başvuruları TR-A veya TR-CIA tarafından belirlenen bir başvuru formu aracılığıyla yapılır. Başvuruda, en az kullanıcının kimlik tespitinin doğru olarak yapılmasını sağlayacak kadar bilgi bulunur.

Kart vermek için aşağıdaki bilgiler gereklidir. Başka kaynaklardan temin edilmediği takdirde, aşağıdaki bilgiler başvuru sırasında alınmalıdır:

- Adı ve soyadı
- Doğum tarihi ve yeri
- İkametgâh adresi
- Vatandaşlık kimlik numarası
- İletişim adresi
- Fotoğraf (eğer geçerli bir fotoğraf dosyası kullanılmıyorsa) (Sürücü kartları dışında zorunlu değil)
- Tercih edilen lisan

Sürücü kartına özel:

- Sürücü belge numarası

Servis kartına özel:

[r31] Servis kartları sadece tüzel kişilere bağlı ve aşağıdaki bilgileri sağlayabilen gerçek kişilere verilir:

- Kullanıcının tam adı ve soyadı;
- Ulusal olarak tanınan kimlik kartında belirtilen doğum tarihi ve yeri, veya kullanıcıyı mümkün olduğunca diğer aynı isimli kişilerden ayırmaya yarayacak öz nitelikler;
- İlgili tüzel kişiliğin veya kurumun tam adı ve hukuki statüsü;

Denetim kartına özel:

[r32] Denetim kartları sadece tüzel kişilere bağlı ve aşağıdaki bilgileri sağlayabilen gerçek kişilere verilir:

- Kullanıcının tam adı ve soyadı;
- Ulusal olarak tanınan kimlik kartında belirtilen doğum tarihi ve yeri, veya kullanıcıyı mümkün olduğunca diğer aynı isimli kişilerden ayırmaya yarayacak öz nitelikler;
- İlgili tüzel kişiliğin veya kurumun tam adı ve hukuki statüsü;

Şirket kartına özel:

[r33] Şirket kartları sayısal takograf cihazlı araçlara sahip veya bulunduran şirketlerin aşağıdaki bilgileri sağlayabilen temsilcilerine verilir:

- Kullanıcının tam adı ve soyadı;
- Ulusal olarak tanınan kimlik kartında belirtilen doğum tarihi ve yeri veya kullanıcıyı mümkün olduğunca diğer aynı isimli kişilerden ayırmaya yarayacak öz nitelikler;
- İlgili tüzel kişiliğin veya kurumun tam adı ve hukuki statüsü;
- İlgili tüzel kişiliğin veya kurumun, herhangi bir ilintili, var olan kayıt bilgisi (örn. şirket kaydı);
- Kullanıcının tüzel kişilik veya kurum ile olan ilgisi.

5.1.2.2 Anlaşma

[r34] Başvuru sahibi kart başvurusu yaparak ve kartı teslim alarak, TR-CIA ile en az aşağıda belirtilen şartları içeren bir anlaşma yapmış olur:

- Kullanıcı, Takograf kartının kullanım şartlarını ve koşullarını kabul eder
- Kullanıcı, TR-CIA tarafından aksi belirtilmedikçe, kartın alınmasından itibaren kullanım süresince aşağıda belirtilen şartlara uymayı kabul eder:
    - Kullanıcı kartının yetkisiz kişilere asla verilmemesini;
    - Kullanıcı tarafından TR-CIA'ya verilen tüm bilginin eksiksiz ve doğru olmasını;

- Kartın kullanım şartlarına uygun bir şekilde bilinçli olarak kullanılmasını.

5.1.2.3 TR-CIA'nın Onay için Şartları – Sürücü kartına özel
[r35] Sürücü kartı sadece başvurunun yapıldığı ülkede daimi ikametgâhı bulunan kişilere verilir.

[r36] TR-CIA, başvuru sahibinin Avrupa Birliği üyesi veya AETR'ye taraf başka bir ülkeden alınmış geçerli bir sürücü belgesinin olmadığından emin olur.

[r37] TR-CIA başvuru sahibinin geçerli uygun sınıfta bir sürücü belgesine sahip olduğunu kontrol eder.

5.1.3 Kart Yenileme – TR-CIA Faaliyeti

[r38] Servis kartlarının geçerlilik süresi üretildiği tarihten itibaren **bir** yıldan daha fazla değildir (AETR 9.1).

[r39] Sürücü kartlarının geçerlilik süresi üretildiği tarihten itibaren **beş** yıldan daha fazla değildir (AETR 11.4.a).

[r40] Şirket kartlarının geçerlilik süresi üretildiği tarihten itibaren **beş** yıldan daha fazla değildir.

[r41] Denetim kartlarının geçerlilik süresi üretildiği tarihten itibaren **iki** yıldan daha fazla değildir.

[r42] TR-CIA, kartların geçerlilik süreleri bitmesine yakın kullanıcılara hatırlatma yapar.

[r43] Yenileme başvurusu Bölüm 5.1.2'de anlatıldığı gibi yapılır.

5.1.3.1 Sürücü Kartları
[r44] Kullanıcı bir yenileme kartı için başvurusunu mevcut kart geçerlilik süresinin bitiminden en az **15** iş günü önce yapar.

[r45] Eğer kullanıcı yukarıdaki şarta uyarsa, TR-CIA mevcut kartın süresi dolmadan önce yeni bir kart verir.

5.1.3.2 Servis Kartları
[r46] Kullanıcı bir yenileme kartı için başvurusunu mevcut kart geçerlilik süresinin bitiminden en az **15** iş günü önce yapar.

[r47] TR-CIA yenileme kartını, eksiksiz olarak başvuruyu aldıktan sonra **5** iş günü içinde verir.

5.1.3.3 Şirket Kartları
[r48] Kullanıcı bir yenileme kartı için başvurusunu mevcut kart geçerlilik süresinin bitiminden en az **15** iş günü önce yapar.

[r49] Eğer kullanıcı yukarıdaki şarta uyarsa, TR-CIA mevcut kartın süresi dolmadan önce yeni bir şirket kartı verir.

5.1.3.4 Denetim Kartları

[r50] Kullanıcı bir yenileme kartı için başvurusunu mevcut kart geçerlilik süresinin bitiminden en az **15** iş günü önce yapar.

[r51] TR-CIA yenileme kartını, eksiksiz olarak başvuruyu aldıktan sonra **5** iş günü içinde verir.

5.1.4 Kart Güncellemesi veya Değişimi – TR-CIA Faaliyeti

[r52] Kullanıcı daimi ikamet ettiği ülkeyi değiştirirse, kendine ait sürücü kartının değiştirilmesini talep edebilir. Eğer mevcut kart geçerli ise, kullanıcı başvurusunun kabul edilmesi için sadece yeni ikametgâh belgesini sunar.

[r53] TR-CIA yeni kartı verirken eski kartı alır ve verildiği Ulusal Otorite' ye gönderir (AETR 11.4.c).

[r54] İkamet edilen ülke değişiminden nedeniyle talep edilen kart değişimi, yeni kart verilirken belirlenmiş şartlara göre geçekleştirilir.

5.1.5 Kayıp, Çalıntı, Zarar Görmüş ve Arızalı Kartların Değişimi – TR-CIA Faaliyeti

[r55] Eğer bir kart kayıp olur veya çalınır ise, kullanıcı bu durumu tutanak ile Polise bildirir ve bu tutanağın bir kopyasını alır. Kayıp kart, kullanıcı tarafından veya kayıp bir kart kendisine ulaştığı zaman Polis tarafından ihbar edilir. Polis en kısa sürede bu durumu TR-CIA'ya bildirir.

[r56] Çalınmış ve kayıp olan kart, bütün Avrupa Birliği üyesi ülkelerce erişilen kara listeye alınır.

[r57] Zarar görmüş ve arızalı kartlar TR-CIA'ya gönderilir, fiziksel olarak imha edilir, elektronik olarak iptal edilir ve kara listeye eklenir.

[r58] Eğer bir kart kayıp olur, çalınır, zarar görür veya arızalanır ise, kullanıcı **7** gün içinde ikame kart için başvuruda bulunur. (AETR 12.1)

[r59] TR-CIA, kullanıcının yukarıdaki belirtilen gereklilikleri sağlaması durumunda, yeni anahtarlar ve sertifikayı içeren ikame kartını eksiksiz olarak başvuruyu aldıktan sonra **5** iş günü içinde verir. (AETR 11.4.a)

[r60] İkame kartının geçerlilik süresi orijinal kart ile aynıdır (AETR Ek 1B: VII). Eğer ikame edilen kartın geçerlilik süresi 6 aydan az kaldıysa, TR-CIA ikame kartı yerine yenileme kartı verebilir.

5.1.6 Başvuru Onayı ve Kayıt – TR-CIA Faaliyeti

[r61] TR-CIA onaylanan başvuruları veri tabanına kaydeder. Buradaki bilgiler TR-CA/TR-CP tarafından sertifika üretimi ve kart kişiselleştirme için kullanılır.

5.1.7 Kart Kişiselleştirme – TR-CP Faaliyeti

Kartlar hem görsel hem elektronik olarak kişiselleştirilir. Bazı durumlarda bu faaliyet, hizmet kuruluşları tarafından gerçekleştirilir, ancak bu, TR-A'nın genel sorumluluğunu azaltmaz.

5.1.7.1 Görsel Kişiselleştirme

[r62] Kartların görsel kişiselleştirmesi AETR Ek 1B, bölüm IV'e uygun olarak yapılır.

5.1.7.2 Kullanıcı Verisinin Karta Yazılması

[r63] Veri, kart tipine bağlı olarak AETR Ek 1B, Alt Ek 2, Kurallar TCS_403, TCS_408, TCS_413 ve TCS_418 göre karta yazılır.

5.1.7.3 Anahtarın Karta Yazılması

[r64] Gizli anahtar, anahtar üretim ortamından hiç çıkarılmadan karta yazılır. Bu ortam, hiçbir kişinin herhangi bir şekilde, üretilmiş gizli anahtarın kontrolünü, sistem tarafından tespit edilmeksizin ele geçirmesini önler. Ayrıca 7.2. donanım anahtarı yönetimine bakınız.

5.1.7.4 Sertifikanın Karta Yazılması

[r65] Sertifikalar, kullanıcılara teslim edilmeden önce karta yazılır.

5.1.7.5 Kalite Kontrol
[r66] Belirlenmiş yöntemler aracılığıyla, kullanıcı kartlarındaki görsel bilgiler ile elektronik bilgilerin birbirleriyle ve geçerli kullanıcıyla eşleşmesi sağlanır. Bu yöntemler UE' de anlatılmaktadır.

5.1.7.6 Dağıtılmamış Kartların İmha Edilmesi
[r67] Kişiselleştirme sırasında zarar gören veya tahrip olan (veya başka nedenlerden dolayı üretimi tamamlanmamış ve dağıtılmamış) kartlar fiziksel olarak imha edilir ve elektronik olarak iptal edilir.

[r68] Tüm imha edilmiş kartlar, iptal listesi veri tabanında tutulur.

5.1.8 Kart Kayıt ve Veri Depolama (DB) – TR-CP ve TR-CIA Faaliyeti

[r69] TR-CP, hangi kartın ve kart numarasının hangi kullanıcıya verildiği bilgisini tutmakla sorumludur. Bu veri TR-CP' den TR-CIA'ya iletilir.

5.1.9 Kullanıcıya Kartın Teslimatı – TR-CP veya TR-CIA Faaliyeti

[r70]

a) Kişiselleştirme, kişiselleştirilen kartın, kullanıcıya tesliminden önce güvenli saklamayı gerektirdiği zamanı en aza indirecek şekilde planlanır. Gece boyunca olan depolamalarda, güvenli saklama için güvenlik önlemleri alınır. Üretim hatalarını da içeren hata yönetimi, teslimatın yapılamaması, kartların zarar görmesi veya kayıp olması hakkında olan yazılı yöntemlere göre işlem yapılır.
b) Kişiselleştirilmiş kartlar en kısa sürede, kullanıcıya gönderiminin veya dağıtımının yapıldığı kontrollü bir alana taşınır.
c) Kişiselleştirilmiş kartlar diğer kartlardan ayrı olarak saklanır.
d) Takograf kartının dağıtımı kayıp riskini en aza indirecek şekilde yapılır.
e) Kartın kullanıcıya teslimatı sırasında kullanıcının kimliği (örn.adı) gerçek bir kişi tarafından kontrol edilir.
f) Kullanıcı, kimlik tespiti için geçerli bir kimlik belgesi sunar.
g) Kartın teslimatı sırasında kullanıcıdan teslim aldığına dair imza alınır.

5.1.10 Doğrulama Kodu (PIN) – TR-CP Faaliyeti

Bu bölüm sadece Servis Kartları için geçerlidir.
[r71] Servis kartları sahip oldukları PIN kodlarıyla, takıldıkları Takograf cihazlarında erişim yetkisi alarak işlem yapar. (AETR Ek 1B, Alt Ek 10: Takograf kartları: 4.2.2)

[r72] PIN kodları en az 4 sayısal karakterden oluşur (AETR Ek 1B, Alt Ek 10: Takograf Cihazı: 4.1.2).

5.1.10.1 PIN Üretimi
[r73] PIN kodları güvenli bir sistemde üretilir, servis kartlarına güvenli bir şekilde aktarılır ve doğrudan PIN zarflarına yazılır. PIN kodları asla, PIN kodları ve kullanıcının arasında bağlantıya izin veren bir biçimde bir bilgisayar sisteminde depolanmaz. PIN üretimi, ITSEC E3, CC EAL4 veya benzer güvenlik kriterlerinin gerekliliklerini karşılayacak biçimde yapılır.

5.1.10.2 PIN Dağıtımı
[r74] PIN kodları posta yoluyla dağıtılır.

[r75] PIN kodları ilgili kartlar ile birlikte dağıtılmaz.

5.1.11 Kart İptali – TR-A/TR-CIA ve TR-CP Faaliyeti

[r76] Kartı ve üzerindeki anahtarları daimi olarak iptal etmek mümkündür. Kart iptal kararı TR-A veya TR-CIA tarafından alınır ve iptal işlemi TR-CP veya Hizmet Kuruluşu tarafından gerçekleştirilir.

[r77] Kartların iptali uygun donanım aracılığıyla yapılır, kart işlevselliğinin sona erdiği ve anahtarların imha edildiği doğrulanır. Ayrıca kart görsel olarak da iptal edilir.

[r78] İptal edilen kartlar, kart veri tabanına kaydedilir ve kart numarası kara listeye eklenir.

5.2 Takograf Cihazı ve Hareket Sensörleri

Şu an veya yakın gelecekte Türkiye'de uygulanabilir değildir.

6 Kök Anahtarlar ve Taşıma Anahtarlarının Yönetimi: Avrupa Kök Anahtarı, Türkiye Anahtarları, Hareket Sensörü Anahtarları, Nakil Anahtarları

Bu bölüm aşağıda verilmiş olan anahtarların yönetimi ile ilgili hükümleri içerir.

- Avrupa Kök Anahtarı - ERCA açık anahtarı (EUR.PK)
- Türkiye Anahtarları, Türkiye imza anahtar çifti (MS.SK, MS.PK)
- Hareket Sensörü Anahtarları (Km_{WC})
- Taşıma Anahtarları (ERCA ve TR-CA arasındaki iletişim için)

ERCA açık anahtarı, Avrupa Birliği üyesi ülkelerin sertifikalarını doğrulamak için kullanılır. ERCA gizli anahtarı asla ERCA'dan dışarı çıkmadığından dolayı bu bölümde konu edilmemiştir.

Türkiye anahtarları, Türkiye imzalama anahtarlarıdır ve ayrıca Türkiye kök anahtarları olarak da adlandırılabilir.

Hareket sensörü anahtarları, servis kartında yer alan simetrik anahtarlardır ve takograf cihazı ile hareket sensörünün karşılıklı tanınmalarını sağlar. TR-CA hareket sensörü anahtarlarını ERCA' dan alır, depolar ve üreticilere dağıtır.

Taşıma anahtarları asimetrik anahtarlardır ve ERCA ile TR-CA arasında bilginin güvenli olarak değişimi için kullanılır.

Eğer ERCA, yukarıda bahsedilen şifreleme anahtarları dışında başka anahtarlara da ihtiyaç duyar ve kullanırsa, bu anahtarlar Takograf Sistemi'nin parçası olarak değerlendirilmez ve bu Politika nın kapsamına girmez.

TR-CA, kendi etki alanının içinde üretilen, kullanılan ve/veya depolanan gizli anahtarların gizliliğinin ve bütünlüğünün korunmasını garanti eder ve etkili olarak bu anahtarların herhangi bir yanlış kullanımını engeller. Bu amaçla, aşağıda verilmiş olan gerekliliklerden birini yerine getiren uygun teknik sistemler kullanılır:

- FIPS 140-2 (veya 140-1) level 3 veya üstü [FIPS],
- CEN Workshop Anlaşması 14176-2 [CEN],
- ISO 15408 [CC] Level E3 veya üstü [ITSEC] ile uyumlu EAL 4 veya üstü ne göre, bu Politika nın gerekliliklerini karşılayan, risk analizi yapılarak, fiziksel ve diğer teknik olmayan güvenlik önlemlerine göre belirlenmiş bir güvenlik hedefi veya koruma profilinin bulunması,
- Aynı güvenlik düzeyini sağlayan güvenlik kriteri.

Aynı şekilde, bu sistemlerin TR-CA' da yeterince güvenliği sağlanmış bir ortamda çalıştırıldığı kanıtlanmak zorundadır. Açık olmayan anahtarların hiçbiri güvenli ortamın dışında bulundurulmaz.

TR-CA, tüm kart sertifikalarını münhasıran Türkiye özel anahtarlarının bulunduğu aynı donanım ile imzalar.

6.1 ERCA Açık Anahtarı

[r98] TR-CA, ERCA açık anahtarını bütünlüğünü koruyarak ve her zaman erişilebilir olmasını sağlayarak saklar. Eğer EUR.PK TR-CP' de depolanacaksa aynı kurala uyulur.

[r99] TR-CP, EUR.PK'nın bütün takograf kartlarına ve takograf cihazlarına yetkileriyle yüklendiğinden emin olur.

6.2 Türkiye Anahtarları

Türkiye anahtarları tüm donanım sertifikalarını imzalamak için kullanılan TR-CA'nın imzalama anahtar çift(ler)idir. Anahtar çifti, açık anahtar (MS.PK), özel veya gizli anahtardan (MS.SK) oluşur. TR-CA açık anahtarı ERCA tarafından onaylanır ancak her zaman TR-CA tarafından üretilir.

[r100] Türkiye gizli anahtarları, Takograf donanım sertifikalarını imzalamak ve ERCA anahtar sertifikasyon talebi (KCR) yapmak dışında kullanılamaz.

6.2.1 Türkiye Anahtarları Üretimi

[r101] Türkiye anahtar çiftinin üretimi aşağıda belirtilen güvenlik kriterlerinden birine sahip olan cihaz aracılığıyla yapılır:

- FIPS 140-2 (veya 140-1) level 3 veya üstü [FIPS];
- CEN Workshop Agreement 14167-2 [CEN];
- ISO 15408 [CC] Level E3 veya üstü [ITSEC] ile uyumlu EAL 4 veya üstüne göre, bu Politika nın gerekliliklerini karşılayan, risk analizi yapılarak, fiziksel ve diğer teknik olmayan güvenlik önlemlerine göre belirlenmiş bir güvenlik hedefi veya koruma profilinin bulunması.

[r102] Anahtar üretim cihazı bağımsız çalışır.

[r103] Kullanılan cihaz ve karşılanan gereklilikler TR-CA UE' de belirtilir.

[r104] TR-CA anahtar çifti üretimi üç ayrı kişinin aktif katılımı ile gerçekleştirilir. Bu kişilerden en az bir tanesi CAA/PA (sertifika üretme otoritesi / kişiselleştirme yöneticisi) rolünde olmalıdır; diğerleri ise güvenilen rollere sahip kişilerden olabilir. (rol tanımları için bakınız bölüm 9.3.1).

[r105] Anahtarlar, anahtar uzunluğu 1024 bit olan RSA algoritması kullanılarak üretilir. (AETR Ek 1B, Alt Ek 11:2.1/3.2).

[r106] ERCA, Türkiye sertifikalarının değişimini hızlıca yapamayacağından, TR-CA imza sertifikaları için, en az iki (2) ve en fazla beş (5) adet anahtar çifti bulundurularak iş sürekliliğini sağlar.

6.2.2 Türkiye Anahtarlarının Geçerlilik Süresi

[r107] Her bir TR-CA gizli anahtarının geçerlilik süresi, ilgili açık anahtarın sertifikasının üretilmesinden itibaren **2** yıldır ve bu anahtarlar bu süreden sonra her hangi bir amaçla kullanılmazlar.

[r108] İlgili açık anahtar, süresiz geçerlidir.

6.2.3 Türkiye Anahtarının Saklanması

[r109] Gizli anahtarlar aşağıdaki özellikleri sağlayan, fiziksel müdahaleler ile içinden bilgi alınmasına karşı dayanıklı bir cihaz tarafından saklanır ve yönetilir:

- FIPS 140-2 (veya 140-1) level 3 veya üstü [FIPS];
- ISO 15408 [CC] Level E3 veya üstü [ITSEC] ile uyumlu EAL 4 veya üstüne göre, bu Politika nın gerekliliklerini karşılayan, risk analizi yapılarak, fiziksel ve diğer teknik olmayan güvenlik önlemlerine göre belirlenmiş bir güvenlik hedefi veya koruma profilinin bulunması.

[r110] TR-CA gizli imzalama anahtarlarına erişim için ikili kontrol zorunludur. Bu yöntem, tek bir kişinin gizli anahtarın saklandığı yere erişim sağlayacak imkânlara sahip olmamasını gerektirir. Bu durum, donanım sertifikaların imzalanmasında iki kontrolün zorunlu olduğu anlamına gelmez.

6.2.4 Türkiye Gizli Anahtarının Yedeklenmesi

[r111] Türkiye gizli imzalama anahtarları en az ikili kontrol gerektiren bir anahtar kurtarma prosedürüne göre yedeklenebilir. Bu prosedür TR-CA EU'da belirtilmiştir.

6.2.5 Türkiye Gizli Anahtarının Emanette Saklamak

[r112] Türkiye gizli imzalama anahtarları emanette saklanmaz.

6.2.6 Türkiye Anahtarlarının Güvenliğinin Yitirilmesi

[r113] Türkiye gizli anahtarlarının güvenliğinin yitirilmesi veya böyle bir şüphenin olması durumunda, kullanıcılar ve TR-CA ve/veya Hizmet Kuruluşlarında bulunan güvenlikten sorumlu kişiler tarafından alınması gereken önlemler, TR-CA EU'da bulunan bir talimatta belirlenir.

[r114] Böyle bir durumda TR-CA en azından aşağıda belirtileni yapar:
− En kısa sürede TR-A, ERCA ve diğer Ulusal Otoriteleri bilgilendirir.

6.2.7 Türkiye Anahtarlarının Kullanımdan Kaldırılması

[r115] TR-CA, her zaman geçerli bir Türkiye imzalama anahtar çiftinin kullanıldığını garanti eden rutinler belirler.

[r116] Türkiye imzalama anahtar çiftinin kullanımdan kaldırılmasının ardından, açık anahtar arşivlenir ve gizli anahtar bir daha kullanılmasını ve tekrar elde edilmesini engelleyecek şekilde TR-CA tarafından imha edilir.

6.3 Hareket Sensörleri Anahtarları

[r117] TR-CA, ERCA'dan hareket sensörü anahtarını KmWC talep eder (AETR Ek 1B, Alt Ek 11:3.1.3). TR-CA hareket sensörü ana anahtarının (Km) veya takograf cihazı hareket sensörü anahtarının (KmVU) yönetimini üstlenmez.

[r120] TR-CA, sadece servis anahtarını servis kartlarına yüklenmesi için TR-CP' ye yönlendirir. TR-CA, Km_{WC} anahtarının sadece ilgili alıcıya ulaşması için gerekli güvenlik önlemlerini alır.

[r121] TR-CP, TR-CA'nın servis anahtarını (Km_{WC}) tüm üretilen servis kartlarına yüklemesi görevini üstlenir. (AETR Ek 1B, Alt Ek 11:3.1.3).

[r122] TR-CA ve/veya TR-CP hareket sensörü anahtarlarının saklanması, kullanımı ve dağıtımı sırasında yüksek güvenilirlikte fiziksel ve mantıksal güvenlik kontrolleri ile korur. Gizli anahtarlar aşağıdaki özellikleri sağlayan, fiziksel müdahaleler ile içinden bilgi alınmasına karşı dayanıklı bir cihaz tarafından saklanır ve yönetilir:

- FIPS 140-2 (veya 140-1) level 3 veya üstü [FIPS];
- ISO 15408 [CC] Level E3 veya üstü [ITSEC] ile uyumlu EAL 4 veya üstüne göre, bu Politika nın gerekliliklerini karşılayan, risk analizi yapılarak, fiziksel ve diğer teknik olmayan güvenlik önlemlerine göre belirlenmiş bir güvenlik hedefi veya koruma profilinin bulunması.

6.4 Taşıma Anahtarları

[r123] Güvenli veri iletişimi için, TR-CP özel asimetrik taşıma anahtarları üretir. TR-CP hareket bu anahtarlarının saklanması, kullanımı ve dağıtımı sırasında yüksek güvenilirlikte fiziksel ve mantıksal

güvenlik kontrolleri ile korur. Gizli anahtarlar aşağıdaki özellikleri sağlayan, fiziksel müdahaleler ile içinden bilgi alınmasına karşı dayanıklı bir cihaz tarafından saklanır ve yönetilir:

- FIPS 140-2 (veya 140-1) level 3 veya üstü [FIPS];
- ISO 15408 [CC] Level E3 veya üstü [ITSEC] ile uyumlu EAL 4 veya üstüne göre, bu Politika nın gerekliliklerini karşılayan, risk analizi yapılarak, fiziksel ve diğer teknik olmayan güvenlik önlemlerine göre belirlenmiş bir güvenlik hedefi veya koruma profilinin bulunması.

6.5 Anahtar Sertifikası Talepleri ve Hareket Sensörü Anahtar Dağıtım Talebi

TR-CA ve ERCA arasında tüm anahtar taşıma işlemleri, ERCA Kök Politikası'nda belirlenen veri taşıma araçları ve protokoller ile gerçekleştirilir. TR-A, TR-CA ve ERCA arasındaki mesajları içeren veri medyasını taşıması için yetkili bir kişiyi görevlendirir.

[r123.1] TR-CA, kendi açık anahtarlarını (MS.PK), ERCA tarafından sertifika üretimi için, Sayısal Takograf Sistemi Avrupa Kök Politikası [ERCA] Ek A'da belirlenen anahtar sertifikası üretim talebi (KCR) protokolünü kullanarak sunar.

[r123.2] TR-CA, ERCA açık anahtarını (EUR.PK), Sayısal Takograf Sistemi Avrupa Kök Politikası [ERCA] Ek B'de belirlenen dağıtım biçiminde tanır.

[r123.3] TR-CA, hareket sensörü ana anahtarlarını, Sayısal Takograf Sistemi Avrupa Kök Politikası [ERCA] Ek D'de belirlenen anahtar dağıtım talebi (KDR) protokolünü kullanarak ERCA'dan talep eder.

[r123.4] TR-CA, anahtar ve sertifika taşıma işlemi için Sayısal Takograf Sistemi Avrupa Kök Politikası [ERCA] Ek C'de belirtilen özelliklerde bir fiziksel veri medyası kullanır.

[r123.5] TR-CA ve TR-CP, ERCA'ya sertifika üretimi ve hareket sensörü anahtarlarının dağıtımı için sunulan anahtarların, anahtar tanımlayıcılarının (KID) ve anahtar uzunluklarının (n) TR-CA ve TR-CP etki alanı içinde tekil olduğunu garanti eder.

[r123.6] TR-CA, gizli anahtarların HSM içinden çıkarılmayacağını ve anahtar sertifikası üretim işlemlerinde taşınmayacağını garanti eder.

[r123.7] TR-CA, gizli anahtarların HSM içinden çıkarılmayacağını ve anahtar simetrik anahtar dağıtım işlemlerinde taşınmayacağını garanti eder.

7 Donanım Anahtarları (asimetrik)

Donanım anahtarları, üretim sürecinde üretilen asimetriktir anahtarlardır ve aşağıda belirtilen takograf sistemi donanımları için TR-CA tarafından sertifikaları üretilir:

- Takograf Kartları
- Takograf Cihazları (Şu an veya yakın gelecekte Türkiye'de uygulanabilir değildir)

Simetrik hareket sensörü anahtarları burada ele alınmamıştır.

7.1 Genel Durum - TR-CP / TR-CA, Hizmet Kuruluşları ve Takograf Cihazı Üreticileri

[r124] Donanımın (Kart ve Takograf Cihazı) başlangıç durumuna getirilmesi, anahtar yükleme ve kişiselleştirme fiziksel olarak güvenli ve kontrollü bir alanda gerçekleştirilir. Bu alana giriş kişiler düzeyinde sıkı denetim ve kontrol altında tutulur. Ayrıca sistemin çalışması için en az iki kişinin mevcudiyet göstermesi gereklidir. Sistemdeki girişlerin ve işlemlerin logu tutulur.

[r125] Anahtar üretim sistemleri, bu politikanın ihlaline neden olabilecek hassas bilgiler içermez.

[r126] Takograf kartları: Kart kişiselleştirme sistemleri, bu politikanın ihlaline neden olabilecek hassas bilgiler içermez.

[r128] **Organizasyonlar (Altyükleniciler, Hizmet Kuruluşları):** Birden fazla Avrupa Birliği üyesi ülke veya Sözleşmeli Taraf adına, anahtar üretimi ve kart kişiselleştirme faaliyetlerinde bulunan organizasyonlar, bu faaliyetleri her biri açıkça birbirinden ayrı olan süreçlerle gerçekleştirir. Her süreç için ayrı bir log tutulur ve ilgili Ulusal Otorite talep üzerine bu loga ulaşır.

[r130] **TR-CA/TR-CP/Hizmet Kuruluşları/Takograf Cihazı Üreticileri:** Kişiselleştirme sisteminin logu ilgili donanım numaralarının, sertifikaların sırasını ve listesini gösteren bir referans içerir. İlgili Ulusal Otorite talep üzerine bu loga ulaşır.

7.2 Donanım Anahtarı Üretimi

[r131] Donanım anahtarları donanım üreticileri veya TR-CP tarafından üretilebilir. (AETR Ek 1B, Alt Ek 11:3.1.1).

[r132] TR-CP, donanım anahtarlarının güvenli bir şekilde üretildiğinden ve donanım gizli anahtarının gizli olarak tutulduğundan emin olur.

[r133] Anahtar üretimi aşağıda belirtilen güvenlik kriterlerinden birine sahip olan cihaz aracılığıyla yapılır:

- FIPS 140-2 (veya 140-1) level 3 veya üstü [FIPS];
- CEN Workshop Agreement 14167-2 [CEN];
- ISO 15408 [CC] Level E3 veya üstü [ITSEC] ile uyumlu EAL 4 veya üstüne göre, bu politikanın gerekliliklerini karşılayan, risk analizi yapılarak, fiziksel ve diğer teknik olmayan güvenlik önlemlerine göre belirlenmiş bir güvenlik hedefi veya koruma profilinin bulunması.

[r134] Anahtarlar, anahtar uzunluğu 1024 bit olan RSA algoritması kullanılarak üretilir (AETR Ek 1B, Alt Ek 11:2.1/3.2).

[r135] Gizli anahtarın üretim prosedürü ve saklama yöntemi, anahtarın üretildiği yerden dışarı çıkarılmasının engellenmesini sağlar. Ayrıca cihaza yüklendikten sonra derhal sistemden silinir.

[r136] Sertifika geçerliliği başlamadan önce, açık anahtarın etki alanı içinde tekil olduğunun garanti edilmesi için gerekli önlemleri almak anahtar üretim biriminin sorumluluğundadır. (Bu şart muhtemelen, anahtar üretim sisteminin doğası gereği rastgele üretim yapması sonucunda, tekil olmayan anahtarların üretim olasılığının olmaması ile sağlanır.)

7.2.1.1 Toplu Anahtar Üretimi

[r137] Kriptografik anahtar üretimi toplu olarak, sertifika talebinden önce veya sertifika talebi ile direkt bağlantılı yapılabilir.

[r138] Toplu üretim, yukarıda belirtilen güvenli gerekliliklerini sağlayan bağımsız çalışan bir donanım ile gerçekleştirilir. Anahtar bütünlüğünün, sertifika üretimi yapılana kadar korunması zorunludur.

7.2.2 Donanım Anahtarının Geçerlilik Süresi

7.2.2.1 Kart Anahtarları

[r139] Bu politikaya göre, üretilmiş sertifikalarla ilişkili bir donanım özel anahtarı, asla ilgili sertifikanın geçerlilik bitişinden sonra kullanılamaz.

7.2.3 Donanım Gizli Anahtarının Korunması ve Saklanması - Kartlar

[r141] TR-CP, kart gizli anahtarının bu politikada belirtilen prosedürlere göre kullanıcıya gönderilen kart tarafından korunduğunu garanti eder.

[r142] Anahtar üretimi ve cihaz kişiselleştirme sırasında gerekmesi durumu hariç, gizli anahtarın kopyaları takograf kartı dışında bir yerde saklanmaz.

[r143] Kart gizli anahtarı hiçbir şekilde ifşa edilmez veya kartın dışında saklanmaz.

7.2.4 Donanım Gizli Anahtarının Korunması ve Saklanması – Takograf Cihazları

Şu an veya yakın gelecekte Türkiye'de uygulanabilir değildir.

7.2.5 Donanım Gizli Anahtarının Emanet Edilmesi ve Arşivlenmesi

[r147] Donanım gizli anahtarları emanet edilmez veya arşivlenmez.

7.2.6 Donanım Açık Anahtarının Arşivlenmesi

[r148] Bütün sertifikalı açık anahtarlar TR-CA tarafından arşivlenir. Sertifikalı açık anahtarlar hakkındaki bilgi TR-CP tarafından da tutulabilir.

7.2.7 Donanım Anahtarlarının Kullanımdan Kaldırılması

[r149] Bir takograf kartının kullanımdan kaldırılmasının ardından, açık anahtar arşivlenir ve gizli anahtar:

- Tekrar elde edilmesini engelleyecek şekilde imha edilir veya
- Tekrar kullanılmasını engelleyecek şekilde saklanır.

8 Donanım Sertifikası Yönetimi

Bu bölüm, sertifika kayıt sürecini de içeren sertifika yaşam döngüsünü, sertifika üretimini, dağıtımını, kullanımını, yenilemesini, iptalini (uygulanabilir ise) ve sertifikanın kullanımdan kaldırılmasını anlatır.

8.1 Veri Girişi

8.1.1 Takograf Kartları

Kart kullanıcıları sertifikalar için başvuru yapmaz, sertifikalar, takograf kartı başvurusu (bölüm 5.1.2) sırasında alınan ve TR-CIA kayıt yetkilisi tarafından kayıt edilen bilgilere istinaden üretilir. Sertifikası üretilecek açık anahtar, anahtar üretim süreci ile oluşturulur.

[r151] TR-CP, girdi verisinin tekil olan Sertifika Sahibi Referans (CHR) bilgisini içerdiğinden emin olur. TR-CA etki alanı içinde CHR'nin tekilliğini doğrular.

[r151.1] Sertifika talep süreci, TR-CP'nin sertifika üretimi için sunulan açık anahtara karşılık gelen gizli anahtara sahip olduğundan emin olur. Bu sırada gizli anahtar, anahtar üretiminin yapıldığı güvenli ortamdan çıkarılmaz.

8.1.2 Takograf Cihazları

Şu an veya yakın gelecekte Türkiye'de uygulanabilir değildir.

8.2 Takograf Kartı Sertifikaları

8.2.1 Sürücü Sertifikaları

[r154] Sürücü sertifikaları, sürücü kartı için başvurmuş, sadece gerekli şartları eksiksiz sağlayan başvuru sahipleri için üretilir.

8.2.2 Servis Sertifikaları

[r155] Servis sertifikaları, servis kartı için başvurmuş, sadece gerekli şartları eksiksiz sağlayan başvuru sahipleri için üretilir.

8.2.3 Denetim Sertifikaları

[r156] Denetim sertifikaları, denetim kartı için başvurmuş, sadece gerekli şartları eksiksiz sağlayan başvuru sahipleri için üretilir.

8.2.4 Şirket Sertifikaları

[r157] Şirket sertifikaları, şirket kartı için başvurmuş, sadece gerekli şartları eksiksiz sağlayan başvuru sahipleri için üretilir.

8.3 Takograf Cihazı Sertifikaları

Şu an veya yakın gelecekte Türkiye'de uygulanabilir değildir.

8.4 Donanım Sertifikalarının Geçerlilik Süresi

[r160] Sertifikaların geçerlilik süresi ilgili donanımlarınkinden daha uzun değildir (bölüm 5):

- Sürücü sertifikalarının geçerlilik süresi **5** yıldan daha uzun değildir (AETR 11.4.a).
- Servis sertifikalarının geçerlilik süresi **1** yıldan daha uzun değildir (AETR 9.1).
- Denetim kurumu sertifikalarının geçerlilik süresi **2** yıldan daha uzun değildir.
- Şirket sertifikalarının geçerlilik süresi **5** yıldan daha uzun değildir.

8.5 Donanım Sertifikası Üretimi

[r161] TR-CA ürettiği sertifikaların münhasırlığının ve bütünlüğünün korunmasını sağlar. Sertifika içeriği AETR Ek 1B, Alt Ek 11'de belirlenmiştir.

8.6 Donanım Sertifikalarının Yenilenmesi ve Güncellenmesi

Donanım Yönetimi bölümüne bakınız (bölüm 5). Sertifikalar ve kartlar aynı geçerlilik sürelerine sahip oldukları için birlikte yönetilirler. Takograf cihazı sertifikaları süresiz geçerlidir veya çok uzun süreli geçerlilik sürelerine sahiptir. Donanımın kullanım süresinin, sertifikanınkinden daha kısa olduğu varsayılmaktadır.

8.7 Donanım Sertifikası ve Bilgisinin Yayımlanması

[r162] TR-CA, tüm sertifika verisini TR-CIA'ya gönderir, böylece sertifikalar ve donanımlar kullanıcıya ulaştırılır.

[r163] TR-CIA, sertifikaların gerektiğinde kullanıcılar ve 3.kişiler tarafından erişilebilir olmasını sağlar.

[r164] TR-CIA, TR-CA UE'nin ilgili kısımları dahil tüm şartların, koşulların ve diğer ilgili bilgilerin tüm kullanıcılarca, 3.kişilerce ve diğer ilgili gruplarca erişilebilir olmasını sağlar.

[r164.1] TR-CA, sertifika durum bilgisinin erişilebilir olmasını sağlar.

8.8 Donanım Sertifikalarının Kullanımı

[r165] Takograf sertifikaları sadece Takograf Sistemi'nde kullanılır.

8.9 Donanım Sertifikalarının İptali

[r166] Sertifikalar iptal edilmez (sertifikaların iptal edilmesinin yerine, geçerli olmayan Takograf donanımı bir kara listeye kayıt edilir ve bu kara liste yol denetimlerinde kontrol edilebilir).

9 TR-CA ve TR-CP Bilgi Güvenliği Yönetimi

Bu bölüm, bu politika tarafından belirlenen bilgi güvenliği önlemlerini anlatır.
Not: Bu bölümün en azından bir kısmı ilgili birimlerin bilgi güvenliği politikalarına göre değiştirilebilir.

9.1 TR-CA ve TR-CP'nin Bilgi Güvenliği Yönetimi

[r167] TR-CA/TR-CP, gerekli ve kabul edilen standartlara uygun idari ve yönetimsel prosedürleri uygular.

[r168] TR-CA/TR-CP, bazı faaliyetlerini alt yükleniciler ile gerçekleştirse bile sertifika hizmetleri ile ilgili tüm konularda sorumludur. Üçüncü tarafların sorumlulukları, TR-CA/TR-CP tarafından açıkça belirlenir ve uygun anlaşmalarla TR-CA/TR-CP tarafından zorunlu tutulan kontrollerin üçüncü taraflarca yapılması garanti edilir. TR-CA/TR-CP, tüm taraflar için uygulama esaslarını belirlemek zorundadır.

[r169] TR-CA/TR-CP, süreçlerinde güvenliği yönetmek için uygun bilgi güvenliği altyapısını her zaman sağlar. Güvenlik düzeyini etkileyen her hangi bir değişiklik TR-A tarafından onaylanır.

[r170] TR-CA/TR-CP ISO 17799'a eş bir güvenlik yönetim sistemi uygular. Resmi sertifikasyon gerekli değildir.

9.2 TR-CA/TR-CP'nin Varlık Sınıflandırması ve Yönetimi

[r171] TR-CA/TR-CP, varlıklarının ve bilgisinin gerekli koruma tedbirleri ile korunduğundan emin olur. Özellikle:

a) TR-CA/TR-CP, iş risklerini değerlendirmek için bir risk analizi yapar, gerekli güvenlik şartlarını ve iş yapış prosedürlerini belirler.
b) TR-CA/TR-CP, tüm bilgi varlıklarının envanterini tutar ve bu varlıklara risk analizi ile tutarlı bir şekilde belirlenen koruma şartları için bir sınıflandırma yapar.

9.3 TR-CA/TR-CP'nin Personel Güvenlik Kontrolleri

9.3.1 Güvenilen Roller

[r172] Bu Politikayı uygulayan bir TR-A/TR-CP, aşağıda listelenen en az üç farklı rolü belirler. İç tehditlere karşı esneklik, en az tavsiye edilen model kadar güçlü ve ilgili roller TR-CA/TR-CP EU'da belirlenmiş ise, görevlerin ayrımı ile ilgili yapılan farklı düzenlemeler kabul edilebilir.

[r173] Tek kişinin, yalnız başına koruma tedbirlerini etkisiz hale getirememesini garanti etmek için, TR-CA/TR-CP sistemlerindeki sorumlulukların, birden fazla roller ve kişiler tarafından yerine getirilmesine ihtiyaç vardır. Sistemlerdeki her hesap, hesap sahibinin rolüne uygun limitli yetkilere sahiptir.

[r174] Tavsiye edilen roller:
a) Sertifika Üretim Otoritesi Yöneticisi ve Kişiselleştirme Yöneticisi (CAA/PA)
b) Sistem Yöneticisi (SA)
c) Bilgi Sistemleri Güvenlik Yöneticisi (ISSO)

[r175] CAA/PA rolü aşağıdakileri içerir:

a) Anahtar üretimini;

b) Sertifika üretimini; (belirlenmiş kurallara göre TR-CA/TR-CP donanımı tarafından işleme alınmak üzere, imzalanmış sertifika taleplerinin üretilmesi)
c) Donanımın kişiselleştirilmesini ve güvenli dağıtımını;
d) TR-CA/TR-CP veri tabanının idamesi ve uygunsuzluk araştırmalarına yardım ile ilgili idari faaliyetleri.

[r176] SA rolü aşağıdakileri içerir:
a) Sistemin güvenli başlatılması ve kapatılması dâhil başlangıç konfigürasyonunu gerçekleştirmek;
b) Tüm yeni hesapların ilk kurulumlarını;
c) İlk ağ başlangıç konfigürasyonunun yapılmasını;
d) Ciddi sistem kayıplarından kurtarma için acil sistem başlatma medyasının yaratılmasını;
e) Güvenli depolama, yedeklerin dağıtımı, çevirim dışı yazılım yükseltmelerini içeren; sistem yedekleme, yazılım yükseltme ve kurtarma faaliyetlerinin gerçekleştirilmesini. Yedekler en az
a) haftada bir kez alınır ve yedek alındıktan sonra sistem kapatılıp açılır, böylece donanım bütünlük kontrolleri gerçekleştirilir.
f) Host adının ve/veya network adresinin değiştirilmesini.

[r177] ISSO rolü aşağıdakileri içerir:
a) CAA/PAA'nın güvenlik ayrıcalıklarının ve erişim kontrollerinin belirlenmesini;
b) Tüm yeni hesaplar için parolalar belirlenmesini;
c) Gerekli sistem kayıtlarının arşivlenmesini;
d) CAA/PA'nın sistem güvenlik politikasına uygun çalıştığını tespit etmek için denetim loglarını gözden geçirilmesini. Haftada en az bir kere denetim logunun gözden geçirilmesini;
e) TR-CA/TR-CP kayıtlarının yıllık envanterini teftiş edilmesini;
f) Türkiye anahtarı üretimine katılmayı.

ISSO, direkt sertifika üretiminde görev almasa bile, diğer kişilerin sorumluluklarının ve bu politikanın gerekliklerini yerine getirmelerini sağlamak için, sistem kayıtlarını veya denetim loglarını inceler.

9.3.2 Rollerinin Ayrımı

[r178] TR-CA/TR-CP'de, yukarıda anlatılan rollerden her birini ayrı kişiler üstlenir ve her görev için **en az bir kişi** belirlenir.

9.3.3 Rol Sahiplerinin Tespiti ve Yetkilendirilmesi

[r179] CAA/PA, SA ve ISSO için kişilerin tespiti ve yetkilendirilmesi uygulama esasları, prosedürler ve bu politikada belirtilen şartlar ile uygun ve tutarlı bir şekilde yapılır.

9.3.4 Kişisel Geçmiş, Yetkinlik, Tecrübe, Klerans Gereklilikleri

[r180] Sertifika ve anahtar bilgisi üretme ile yönetme faaliyetlerini gerçekleştiren CAA/PA (Sertifika Üretme Otoritesi / Kişiselleştirme Yöneticisi) kritik bir pozisyondur. CAA/PA rolünü üstlenen kişi, tartışılmaz sadık, güvenilir ve dürüst olmalı, günlük aktivitelerinde güvenlik bilinci ve farkındalığı göstermiş olmalıdır.

[r181] En azından tüm CAA/PA ve ISSO (Bilgi Sistemi Güvenlik Yöneticisi) dâhil olmak üzere, hassas pozisyonda olan tüm TR-CA/TR-CP personeli:
a) CAA/PA ve ISSO olarak görevleri ve sorumlulukları ile çakışan başka görevlere atanmazlar;
b) Önceki görevlerinden ihmalkârlık ve yetersiz performans sonucu alınmamış olmalıdır;
c) Görevlerine uygun eğitim alırlar.

[r182] TR-CA/TR-CP her zaman, yetkinliği, seviyesi, sabıkasının olmaması ve kredi riski kontrol edilen personele sahip olur. Bu gereklilikler uygulanabilir UE'de belirtilmiş olmalıdır.

9.3.5 Eğitim Gereklilikleri

[r183] Personel rol ve iş için gerekli eğitimi alır.

9.4 CA ve Kişiselleştirme Sistemlerinin Sistem Güvenlik Kontrolleri

[r184] TR-CA/TR-CP, sistemlerin minimum hata riskiyle güvenli ve doğru işletildiğinden emin olur. Özellikle:

a) Sistemlerin ve bilginin bütünlüğü virüslere, zararlı ve yetkisiz yazılımlara karşı korunur;
b) Güvenlik olayları ve arızalardan kaynaklı zararlar, olay raporlaması ve tepki prosedürleriyle minimize edilir;

[r185] Sertifika Üretme Otoritesi Sistemi (CAS) ve Kişiselleştirme Sistemi, bu politikada veya ilgili UE'de belirtilen rollerin ayrımını gerçekleştirmek için gerekli sistem güvenlik kontrollerini sağlar.

[r186] Güvenlik kontrolleri, TR-CA'nın özel üretim anahtarlarının kullanımını etkileyen tüm hareketlere ve işlemlere, erişim kontrolü ve kişisel seviyeye kadar izlenebilirlik sağlar.

[r187] Hizmet Kuruluşlarınca kullanılan bilgisayar sistemleri için konulan sistem güvenlik kontrolleri, atanmış kuruluşun rolüne bağlıdır. Kartlara sertifikaları yükleyen veya bu kartları başlangıç durumuna getiren CAA/PA (sertifika üretme otoritesi/kişiselleştirme yöneticisi) rollerini üstlenen kuruluşlar, TR-CA/TR-CP tarafından kendileri için zorunlu tutulan gereklilikleri sağlarlar.

9.4.1 Özel Bilgisayar Güvenliği Teknik Gereklilikleri

[r188] TR-CA'nın gizli sertifika üretme anahtarlarını işleten sistemin başlatılması, her biri için sistem tarafından güvenli olarak kimliği doğrulanmış ve izin verilmiş en az iki operatörün işbirliğini gerektirir.

9.4.2 Bilgisayar Güvenlik Sınıflandırması

[r189] CA ve kişiselleştirme sistemleri, bu bölümde yer alan tüm gereklilikleri sağladığı takdirde resmi sınıflandırma yapmayı şart koşmaz.

9.4.3 Sistem Geliştirme Kontrolleri

[r190] TR-CA/TR-CP, değişikliğe karşı korunan güvenilir sistemler ve ürünler kullanır.

[r191] Güvenlilik gerekliliklerinin analizi, TR-CA/TR-CP tarafından veya BT sistemlerine güvenlik alt yapısı kurulmasını sağlamak için TR-CA/TR-CP adına üstlenilen her hangi bir sistem geliştirme projesinin tasarım ve gereklilik belirleme safhasında yapılır.

[r192] Değişim kontrol prosedürleri, yeni sürümler, değişiklikler ve her hangi bir işletim yazılımını onaran acil durum yazılımları için kullanılır.

9.4.4 Güvenlik Yönetim Kontrolleri

[r193] Sistem rolleri (bölüm 9.3.1) uygulanır ve yürütülür.

9.4.5 Ağ Güvenliği Kontrolleri

[r194] Kontroller (örn. güvenlik duvarları), TR-CA/TR-CP'nin iç ağ etki alanlarını, üçüncü taraflarca erişilebilen dış ağ etki alanlarından korumak için kullanılır.

[r195] Hassas bilgi, güvenli olmayan ağ üzerinden iletileceği zaman korunur.

9.5 Güvenlik Denetim Prosedürleri

Bu bölümdeki güvenlik denetleme prosedürleri; anahtarların, sertifikaların ve donanımların, bu politika koşullarında gerçekleştirilen üretim süreçlerini etkileyen tüm bilgisayar ve sistem bileşenleri için geçerlidir.

9.5.1 Kaydedilen Olayların Tipi

[r196] TR-CA/TR-CP bilgisayarı/sistemi ile ilgili aşağıdaki işlemlerin güvenlik denetleme amacıyla logu tutulur:

a) Hesapların oluşturulması (ayrıcalıklı veya değil),
b) Talep edilen hesabı, talebin tipini, işlemin tamamlandığını veya tamamlanmadığını gösteren bilgiyi ve tamamlanmayan işlemin nihai nedenini içeren kayıtlar dâhil işlem sonuçları,
c) Yeni yazılımların veya güncellemelerin yüklenmesi,
d) Tüm yedeklerin saat, tarih ve diğer tanımlayıcı bilgileri,
e) Sistemin kapatılması ve yeniden açılması,
f) Tüm donanım yükseltmelerinin saat ve tarihi,
g) Denetleme loglarının saat ve tarihi,
h) Arşiv hareketlerinin saat ve tarihi.

9.5.2 Denetimin Logunu İşleme Sıkılığı

[r197] Log düzenli olarak işlenir ve zararlı içeriğe karşı analiz edilir. Log prosedürü UE'de belirtilir.

9.5.3 Denetim Logunun Saklanma Süresi

[r198] Denetim logu en az **7** yıl saklanır.

9.5.4 Denetim Logunun Korunması

[r199] Denetim loglarının uygun bir biçimde bütünlüğü korunur. Tüm girdilere tek tek zaman damgası eklenir (sistem zamanı yeterlidir).

[r200] Denetim logları en az aylık olarak doğrulanır ve birleştirilir. Bahsedilen doğrulama ve birleştirme işlemi için, SA veya ISSO rollerinde (bakınız bölüm 9.3.1) en az iki kişi bulunur.

9.5.5 Denetim Logları Yedekleme Prosedürleri

[r201] Birleştirilmiş logun iki kopyası oluşturulur ve fiziksel olarak güvenli ayrı ortamlarda tutulur.

[r202] Denetim logu, saklama süresince incelenmesini imkan veren bir şekilde depolanır.

[r203] Denetim logu yetkisiz erişimden korunur.

9.5.6 Denetim Derleme Sistemi (İç veya Dış)

[r204] Sadece iç denetim derleme sistemi zorunludur.

9.6 Kayıtların Arşivlenmesi

9.6.1 TR-CIA Tarafından Kaydedilen Olayların Tipi

[r205] Kayıtlar, aşağıda belirtilenler ile sınırlı olmamak üzere TR-CIA'nın sahipliğinde bulunan ilgili tüm kanıtları içerir:

a) Sertifika talepleri ve TR-CA/TR-CP, kullanıcılar ve yönetim arasında gerçekleşen tüm ilgili mesajlaşmaları,
b) Sertifikalar ve kartlar için kullanıcının başvurusunda, başvuruyu kabul eden sorumlu kişininin kimlik bilgilerini de içeren imzalı kayıt anlaşmaları.
c) Kart teslimatının yapıldığına dair imzalı kabul dokümanını,
d) Sertifikalar ve ilgili kartlar hakkında sözleşmeli anlaşmaları,
e) Sertifika yenilemeleri ve kullanıcı ile gerçekleştirilen tüm mesajlaşmaları,
f) İptal talepleri ve talebin sahibi ile gerçekleşen tüm kayıtlı mesajlaşmaları,
g) Yürürlükteki ve önceki uygulanmış politika dokümanlarını.

9.6.2 TR-CA/TR-CP Tarafından Kaydedilen Olayların Tipi

[r206] Kayıtlar, aşağıda belirtilenler ile sınırlı olmamak üzere TR-CA/TR-CP'nin sahipliğinde bulunan ilgili tüm kanıtları içerir:

a) Üretilmiş sertifikaların içeriği.
b) TR-CA/TR-CP'nin EU'ya uyumlu çalıştığını tetkik etmek için gerçekleştirilen yıllık denetlemelerin kayıtlarını içeren denetleme bülteni,
c) Yürürlükteki ve önceki uygulanmış politika dokümanları ve ilgili UE'leri.

[r207] TR-CA/TR-CP veya Hizmet Kuruluşu personeli (CAA/PA) tarafından yapılan, sayısal olarak imzalanmış tüm taleplerin kayıtları; her talepten sorumlu yöneticinin kimlik bilgisi ile birlikte kayıt saklandığı sürece talebin inkâr edilemezlik kontrolü için gerekli tüm bilgileri içerir.

9.6.3 Arşiv Saklama Süresi

[r208] Arşiv UE'de belirtilen süre boyunca değiştirilme veya tahrip edilmeye karşı saklanır ve korunur.

9.6.4 Arşiv Bilgisine Ulaşma ve Bilgiyi Doğrulama Prosedürleri

[r209] TR-CA/CP, bölüm 3.4'de belirtilen gizliliğin sağlanması hakkında olan gerekliliklere uygun faaliyet gösterir.

[r210] Kişisel işlemlerin kayıtları, işleme dâhil olan herhangi bir kullanıcının veya yetkili temsilcilerinin talep etmesi durumunda verilebilir.

[r211] TR-CA/TR-CP talep üzerine, bölüm 11.5'e göre TR-CA/TR-CP'nin UE ile uyumluluğu hakkında oluşturulan dokümantasyonu erişilebilir yapar.

[r212] Duruma göre, arşivden kayıt çıkarma maliyetini karşılamak için bir işlem ücreti talep edilebilir.

[r213] TR-CA/TR-CP, kendi faaliyetleri kesintiye uğrasa, askıya alınsa veya tamamen sona erdirilse bile, arşivin erişilebilir olmasını ve arşiv bilgisinin saklama süresi boyunca okunabilir bir biçimde kayıt altında tutulmasını sağlar.

[r214] TR-CA/TR-CP, hizmetlerinin kesintiye uğraması, askıya alınması veya tamamen sona erdirilmesi durumunda, tüm müşterilerine arşivin sürekli erişilebilir olmasını sağlayacağına dair bir duyuruda bulunur. Arşivlenmiş bilgiye erişmek için yapılacak tüm talepler, hizmetlerinin tamamen sona erdirilmesinden önce TR-CA/TR-CP'ye veya TR-CA/TR-CP tarafından belirlenen bir kuruma gönderilir.

9.7 TR-CA/TR-CP İş Sürekliliği Planı

[r215] TR-CA/TR-CP'nin bir iş sürekliliği planı (BCP) vardır. Bu plan (sınırlı olmamak ile birlikte) aşağıda belirtilen olayları içerir:
- Anahtar güvenliğinin yitirilmesi
- Örneğin çalınma, yangın, donanım veya yazılım arızaları sonucunda meydana gelen çok büyük veri kayıpları
- Diğer sistem hataları

9.7.1 Türkiye Anahtarlarının Güvenliğinin Yitirilmesi

Türkiye anahtarlarının güvenliğinin yitirilmesi bölüm 6'da anlatılmıştır.

9.7.2 Diğer Felaket Kurtarma Durumları

[r216] TR-CA/TR-CP ve altyükleniciler büyük sistem hatalarının etkisinden korunmak ve zararları mümkün olduğunca azaltmak için yöntemler belirlerler. Bu yöntemler, güvenli ve uzaktan yedek verinin depolanması, BCP'de detayları verilen, işler veri onarma prosedürleri ve benzeri konuları içerir.

9.8 CA ve Kişiselleştirme Sistemlerinin Fiziksel Güvenlik Kontrolü

[r217] Fiziksel güvenlik kontrolleri, TR-CA veya TR-CP'nin donanım ve yazılımlarına kontrollü erişim için uygulanır. Bu kontrol, çalışma istasyonlarını, CA ve kişiselleştirme donanımın diğer bileşenlerini ve her hangi bir harici şifreleme donanım modülünü veya kartını içerir. Bu alan (veya alanlara) yapılan tüm fiziksel girişlerin logu tutulur.

[r218] Sertifikaları imzalamak için kullanılan Türkiye anahtarları, UE'de belirtildiği gibi fiziksel ve elektronik korunarak saklanır.

[r219] Ayrıca, TR-CA/TR-CP'nin tesisinde yedek ve dağıtım medyalarını; kayıplara, fiziksel müdahalelere veya saklanan bilginin yetkisiz kullanımına karşı yeterli düzeyde koruyacak şekilde saklamak için bir mekân bulunur. Veri kurtarma ve önemli bilgi arşivleri için yedekleme yapılır. Yedekleme medyası, TR-CA/TR-CP sistemlerinin bulunduğu tesisten başka bir yerde de, asıl tesis bir doğal felakete maruz kaldığında sistemde onarma, düzeltme ve kurtarma yapılabilmesi için saklanır.

[r220] Her **24** saatte en az bir kere, TR-CA/TR-CP'nin ana donanımın bulunduğu tesisin güvenlik kontrolü yapılır. Eğer tesis sürekli çalışılan bir yer ise, sistemlerin ve ilgili şifreleme cihazlarının/kartlarının, kullanımda olmadıklarında güvenli olarak saklanmasını sağlamak için, her vardiya değişiminde, fiziksel güvenlik sistemlerinin (örn. kapı kilitleri ve alarmlar) düzgün çalıştığını, zorla giriş veya yetkisiz erişimin olmadığını içeren görsel bir kontrol yapılabilir.

9.8.1 Fiziksel Erişim

[r221] Türkiye anahtarlarının ve kullanımını sağlayan araçların bulunduğu fiziksel alana giriş için, her birinin bu bölgeye giriş yetkisi olan, en az **2** kişinin aynı anda mevcudiyet göstermesi gerekmektedir.

[r222] TR-CA/TR-CP'nin diğer tesislerine erişim, bölüm 9.3.1'de belirtilen rollerden birini üstlenen personel ile sınırlıdır. Erişim kontrolü, sistemlerin bulunduğu odaya giriş yetkisi bulunan personeli gösteren bir erişim kontrol listesi aracılığıyla yapılabilir. Erişim kontrol listesinde yer almayan bir kişiye, listede bulunan bir kişi tarafından refakat edilir. Eğer bir alan için erişim kontrolü yapmak mümkün değilse, CA ve kişiselleştirme ile ilgili malzemelerin kullanılmadıklarında güvenli bir odada veya depolama alanında kilitli olarak tutulmasının sağlanması kabul edilebilir.

10 TR-CA veya TR-CP Hizmetlerine Son Verilmesi

10.1 Hizmetlerin Tamamen Sonlandırılması - TR-A Sorumluluğu

TR-CA veya TR-CP'nin hizmetlerinin tamamen sonlandırılması, ilgili organizasyon birimin tüm hizmetlerin daimi olarak durdurulmuş olmasıdır. Bu durum hizmetin bir organizasyondan diğerine devri veya TR-CA hizmetin, eski Türkiye anahtar çiftinden yeni Türkiye anahtar çiftine veya ERCA anahtarına geçişi değildir.

[r223] TR-A aşağıda verilmiş işlerinin yapılmasını sağlar. Not: TR-CA/TR-CP hizmetlerine son verilmesi, hem Türkiye'nin takograf sisteminden çıkması veya CA'lar veya benzeri otoriteler olmadan çalışamayacağından dolayı tüm takograf sisteminin faaliyetlerinin sonlandırılması anlamına gelir.

[r224] TR-A/TR-CP hizmetlerini sona erdirmeden önce en azından aşağıda verilmiş olan prosedürler tamamlanmak zorundadır:

a) Tüm kullanıcılar ve TR-CA/TR-CP ile anlaşması olan veya başka şekilde kurulmuş ilişkisi olan taraflar bilgilendirilir.
b) Hizmetlerine son vermeden en az **3** ay önce bu bilgiyi herkesin erişimine açık bir hale getirir.
c) Sertifika üretim sürecinde TR-CA/TR-CP adına faaliyet gösteren alt yüklenicilerin tüm yetkilerini kaldırır.
d) TR-CA/TR-CP, arşiv kayıtlarının saklanma süreleri boyunca muhafaza edilmesi yükümlülüğünün devri için gerekli girişimleri yapar.

10.2 TR-CA veya TR-CP Sorumluluğunun Devri

TR-CA veya TR-CP'nin sorumluluk devri, TR-A'nın öncekilerin yerine yeni bir TR-CA veya TR-CP görevlendirmeyi tercih ettiğinde gerçekleşir.

[r225] TR-A, sorumlulukların ve varlıkların düzgün bir şekilde devredilmesini sağlar.

[r226] Önceki TR-CA, tüm kök anahtarlarını TR-A'nın kararlaştıracağı bir şekilde yeni TR-CA'ya devreder.

[r227] Önceki TR-CA, devredilmeyen anahtarların kopyalarını yok eder.

11 Denetim

[r228] TR-A, TR-CA ve TR-CP denetimlerinin yapılmasını sağlar.

11.1 Uyumluluk Denetiminin Sıklığı

[r229] Bu politikaya göre faaliyet gösteren TR-CA/TR-CP, politikaya uygun olarak faaliyet gösterdiğine dair denetlenir. TR-CA/TR-CP ilk olarak, onaylanan Politika kapsamında faaliyetlerine başladıktan 12 ay içinde denetlenir. Yapılan denetimde uygunsuzluk bulunmadığı zaman, bir sonraki denetim 24 ay içinde gerçekleştirilir. Yapılan denetimde uygunsuzluk bulunduğu zaman, bir sonraki denetim 12 ay içinde gerçekleştirilir.

11.2 Denetleme Kapsamındaki Konular

[r230] Denetleme TR-CA/TR-CP'nin uygulamalarını kapsar (UE'lerine göre).

[r231] Denetleme TR-CA/TR-CP'nin bu politika ile uyumluluğunu kapsar.

[r231.1] Denetleme ERCA-CP 5.3'te belirlenen gereklilikleri kapsar.

[r232] Denetleme Hizmet Kuruluşlarının faaliyetlerini de kapsar.

11.3 Denetim Yapan Kurum

[r233] TR-A, 3.kişilerin uygulamaya güvenlerinin artması için, harici bir sertifikasyon veya akreditasyon kurumundan TR-CA/TR-CP UE'sinin onayı için danışmalık hizmeti alabilir. Aksi durumlarda denetimi TR-A gerçekleştirir.

11.4 Kusur Sonucu Alınacak Tedbirler

[r234] Eğer denetimde kusurlar bulunursa, TR-A durumun ciddiyetine göre uygun tedbirleri alır.

11.5 Sonuçların Bildirilmesi

[r235] Güvenlik durumu düzeyi hakkındaki denetim sonuçlarına talep olduğu takdirde erişilebilir. Denetim raporlarının asıllarına erişim, bilinmesi gereken prensibine göre gerçekleştirilir.
[r235.1] TR-A denetim sonuçlarını, TR-A yükümlülüklerini yerine getirmek için gerekli olan düzeltici faaliyetleri belirleyen ve bu faaliyetlerin gerçekleştirilme takvimini de içeren bir raporda verir. Rapor İngilizce olarak ERCA'ya gönderilir.

12 Politika Değişim Prosedürleri

12.1 Bildirimde Bulunulmadan Yapılabilecek Değişiklikler

[r236] Bildirimde bulunmadan yapılabilecek değişiklikler sadece aşağıda belirtilen değişikliklerdir.

a) Yazım veya baskı hatası düzeltmeleri
b) İletişim bilgilerindeki değişiklikler

12.2 Bildirimde Bulunularak Yapılabilecek Değişiklikler

12.2.1 Bildirim

[r237] Bu sertifika politikasında herhangi bir madde, **90** gün önceden bildirim yapılarak değiştirilebilir.

[r238] Politikadan sorumlu organizasyonun (TR-A) değerlendirmesiyle, bu politikayı kullanan kullanıcılarının veya üçüncü kişilerin büyük bir bölümünü ciddi boyutta **etkilemeyecek** değişiklikler **30** gün önceden bildirim yapılarak gerçekleştirilebilir.

12.2.2 Yorum Süresi

[r239] Değişiklikten etkilenecek kullanıcılar, ilk bildirim yapıldıktan itibaren **15** gün içinde politika yönetim organizasyonu ile yorumlarını dosyalayabilirler.

12.2.3 Bilgilendirme Yapılacak Taraflar

[r240] Bu politikaya yapılan değişiklikler hakkındaki bilgi aşağıda verilen taraflara gönderilir:

- ERCA;
- TR-CIA, TR-CA ve TR-CP, alt yükleniciler dâhil;
- UN-ECE Transport Division.

12.2.4 Final Değişikliğinin Bildirim Süresi

[r241] Eğer teklif edilen değişiklik yorumlar sonucunda güncellendiyse, güncellenmiş teklif edilen değişikliğin yürürlüğe girmesi için en az 30 gün süre verilir.

12.3 Politikanın Yeniden Onaylanmasını Gerektiren Değişiklikler

[r242] Eğer TR-A organizasyonu tarafından kararlaştıran Politika değişikliği, önemli sayıda politika kullanıcısını ciddi boyutta etkiliyorsa, TR-A revize edilen Politikayı ERCA'ya onay için sunar.

13 Referanslar

[BPM] Digital Tachograph Card Issuing Best Practice Manual. Card Issuing Group, 16 November 2001. - owned by the European Commission.

[CC] Common Criteria. ISO/IEC 15408-1:2009 "Information technology - Security techniques - Evaluation criteria for IT security – Part 1: Introduction and general model".

[CC] Common Criteria. ISO/IEC 15408-2:2008 "Information technology - Security techniques - Evaluation criteria for IT security – Part 2: Security functional components".

[CC] Common Criteria. ISO/IEC 15408-3:2008 "Information technology - Security techniques - Evaluation criteria for IT security – Part 3: Security assurance components".

[CEN] CEN Workshop Agreement 14167-2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)

[ETSI 102 042] ETSI TS 102 042. Policy requirements for certification authorities issuing public key certificates

[FIPS] FIPS PUB 140-2 (May 25, 2001): "Security Requirements for Cryptographic Modules". Information Technology Laboratory, National Institute of Standards and Technology (NIST)

[ISO 17799] BS ISO/IEC 17799: 2005. Information technology -- Code of practice for information security management.

[CSG] Common Security Guideline, Card Issuing Project. – owed by the European Commission

[ERCA] Digital Tachograph System European Root Policy, Version 2.1; European Commission Joint Research Center Publication 53429; 28th July 2009; published at http://dtc.ec.europa.eu.

[AETR] European Agreement Concerning the Work of Crews of Vehicles Engaged in International Road Transport (AETR) concluded at Geneva on 1 July 1970

[AETR] Implementation of the AETR - Project plan for AETR Contracting Parties (ECE/TRANS/SC.1/2006/9)

14 Sözlük/Tanımlar ve Kısaltmalar

14.1 Sözlük/Tanımlar

Açık Anahtar: Açık anahtar şifreleme teknikleri için kullanılan asimetrik bir anahtar çiftinin açık olan kısmıdır. Açık anahtar genellikle sayısal imzaları doğrulamak veya gizli anahtarın sahibine mesaj şifrelemek için kullanılır.

CA Politikası: Anahtarların, sertifikaların, belli bir topluluk için olan donanımların ve/veya ortak güvenlik gerekliliklerini sağlayan uygulama sınıfının uygulanabilirliğini gösteren adlandırılmış kurallar topluğudur.

Donanım: Takograf Sistemi'ndeki donanımlar: Takograf Kartları, VU(takograf cihazı) ve hareket sensörleri

Gizli Anahtar: Açık anahtar şifreleme teknikleri için kullanılan asimetrik bir anahtar çiftinin gizli olan kısmıdır. Gizli anahtar genellikle sayısal imzaları imzalamak veya mesajların şifrelerini çözmek için kullanılır.

Hareket Sensörü Anahtarı: Hareket Sensörü ve VU'nun birbirlerini karşılıklı tanımalarını sağlamak için kullanılan simetrik bir anahtar.

Hizmet Kuruluşu: Alt yüklenici olarak TR-CA adına görev yapan kuruluş.

Bu dokümanda:
İmzalanmış: Bu politikanın imza gerektirdiği yerde, gereklilik güvenli ve doğrulanabilir sayısal imza ile sağlanır.

Kart Sahibi: Takograf kartının sahibi ve kullanıcısı olan kişi veya kurum. Bunlar sürücüler, şirket temsilcileri, servis çalışanları ve denetim kurumu personelleridir.

Kart/Takograf Kartları: Entegre Devre ile donatılmış kart, bu politikada "**IC-Kart**" ve "**Akıllı Kart**" terimlerinin kullanımı ile eş değerdir.

Kullanıcı: Kullanıcılar; donanım kullanıcıları, kart için **Kart Sahipleri** veya takograf kartları/hareket sensörleri için **üreticilerdir**.

RSA Anahtarları: RSA, Takograf sistemindeki asimetrik anahtarlar (PKI) için kullanılan şifreleme algoritmasıdır.

Sertifika Üretim Otoritesi Sistemi (CAS): Sertifika (kullanıcı) verisinin CA'nın gizli imzalama anahtarı ile imzalanarak sertifikaların üretildiği bilgisayar sistemidir.

Sertifika Üretim Uygulama Esasları (CPS): Sertifika üretim otoritesinin sertifika üretiminde kullandığı ve asıl CA Politikası ile bağlantılı olan uygulamalar esaslarıdır. Bu politikada CPS yerine, daha geniş bakış açısına sahip olduğundan, anahtarlar, sertifikalar ve donanımlar arasındaki bağlantıları kurduğundan dolayı Uygulama Esasları kullanılmıştır.

Sertifika: Genel bir çerçevede bir sertifika, sertifika içindeki bilginin doğru olduğunu ve sertifika üretimi yapılmış açık anahtarın sahibinin, ilgili gizli anahtara sahip olma hakkını kanıtlayabileceğini tasdik eden, sertifikayı veren tarafın bağlayıcı imzasını içeren bir mesaj yapısıdır.

Takograf Kartları/Kartlar: Takograf sisteminde dört farklı tip akıllı kart kullanılır: Sürücü kartı, Şirket kartı, Servis kartı, Denetim kartı.

Uygulama Esasları (UE): Takograf süreçlerinde kullanılan güvenlik uygulama esaslarıdır. UE standart PKI dokümanı olan CPS'e benzer.

Üretici/Donanım Üreticisi: Takograf donanımlarının üreticileri. Sistemde ayrı rolleri olduğundan dolayı, bu politikada sıklıkla takograf cihazı ve hareket sensörü üreticileri için kullanılmıştır.

Yazılmış: Bu politikanın bilginin yazılı olmasını gerektirdiği yerde, eğer oradaki bilgi erişilebilir ve böylece ilgili taraflarca kullanılabilir ise, bu gereklilik bir veri mesajı ile sağlanır.

14.2 Kısaltmalar

CA Sertifika Üretim Otoritesi
CAA/PA Sertifika Üretim Otoritesi Yöneticisi/Kişiselleştirme Yöneticisi
CAS Sertifika Üretim Otoritesi Sistemi
CIA Kart Verme Otoritesi
CC Ortak Kriter
CP Kart Kişiselleştirme Organizasyonu
CPS Sertifika Uygulama Esasları
ERCA Avrupa Kök CA
ISSO Bilgi Sistemi Güvenlik Yöneticisi
ITSEC Bilgi Teknolojisi Güvenlik Değerlendirme Kriteri
KG Anahtar Üretimi
MS Avrupa Birliğine Üye Ülke
MSA Avrupa Birliğine Üye Ülke Otoritesi
MSCA Avrupa Birliğine Üye Ülke CA
PIN Kişisel Tanımlama Numarası
PKI Açık Anahtar Altyapısı
RSA Özel bir Açık Anahtar Algoritması
SA Sistem Yöneticisi
PS Uygulama Esasları
TR-A Türkiye Ulusal Otoritesi
TR-CA Türkiye Sertifika Üretim Otoritesi
TR-CIA Türkiye Kart Verme Otoritesi
TR-CP Türkiye Kart Kişiselleştirme Organizasyonu
VU Takograf Cihazı
VUP VU Kişiselleştirme Organizasyonu

15 ERCA Politikası ile Karşılaştırma Tablosu

TR-A Politikası ile ilgili gereklilikler ERCA Politikası § 5.3'te düzenlenmiştir. Aşağıdaki tablo, ERCA Politikası'nda düzenlenen gereklilikler ve TR-A Politikası'ndaki gereklilikler arasındaki bağlantıyı sağlar.

Sıra	ERCA Politikası Referansı	Gereklilik	TR-A Politikası Referansı
1	§ 5.3.1	Üye Ülke Otoritesi (MSA) politikası faaliyetlerden sorumlu kişileri belirlemelidir.	§1.1 Sorumlu Organizasyon
2	§ 5.3.2	Cihaz anahtar sertifikasyonu ve hareket sensörü anahtar dağıtımı için kullanılan Ulusal Sertifika otoritesi anahtar çiftleri, aşağıdaki özelliklerden birine sahip bir cihazda üretilmeli ve saklanmalıdır. • FIPS 140-2 (veya FIPS 140-1) seviye 3 veya üstü [10] içeriğinde belirtilen gereklilikleri sağlamak üzere belgelendirilmiş; • CEN Workshop Agreement 14167-2 [11] içeriğinde belirtilen gerekliliklerle uyumlu olduğuna dair belgelendirilmiş; • ISO 15408'e [12] göre EAL4 veya üstü, ITSEC'e [13] göre seviye E3 veya üstü veya eşdeğer güvenlik kriterlerine uygunluğu temin edilmiş bir güvenilir sistem. Bu değerlemeler bir koruma profiline ya da güvenlik hedefine yönelik olmalıdır. • Eşdeğer bir güvenlik seviyesi sağladığı gösterilmiş.	§6.2.1 Türkiye Anahtarları Üretimi §6.3 Hareket Sensörleri Anahtarları §6.4 Taşıma Anahtarları §6.5 Anahtar Sertifikası Talepleri ve Hareket Sensörü Anahtar Dağıtım Talebi
3	§ 5.3.3	Üye Ülke Anahtar Çifti üretimi, fiziksel güvenliği sağlanmış bir ortamda, güvenilir rollerdeki personel tarafından, en az iki kişinin kontrolü altında gerçekleştirilmektedir.	§6 Kök Anahtarlar ve Taşıma Anahtarlarının Yönetimi: Avrupa Kök Anahtarı, Türkiye Anahtarları, Hareket Sensörü Anahtarları, Nakil Anahtarları [paragraf 8] §6.2.1 Türkiye Anahtarları Üretimi [r104]
4	§ 5.3.4	Üye Ülke Anahtar Çiftleri, ERCA tarafından sertifika üretimi yapıldıktan sonra en çok iki yıllık bir süre boyunca kullanılmalıdır.	§6.2.2 Türkiye Anahtarlarının Geçerlilik Süresi
5	§ 5.3.5	Üye Ülke Anahtar Çiftlerinin üretimi için, ERCA tarafından sertifika üretimi yapılması için gerekli	§6.2.1 Türkiye Anahtarları Üretimi [r106]

		olan bir aylık işlem süresi dikkate alınmalıdır.	
6	§ 5.3.6	Üye Ülke Otoritesi (MSA), Üye Ülke Sertifika Üretim Otoroitesi (MSCA) açık anahtarlarını, Ek A'da tanımlanan anahtar sertifikalandırma talebi (KCR) protokolünü kullanarak ERCA'ya sertifika üretimi için göndermelidir.	§6.5 Anahtar Sertifikası Talepleri ve Hareket Sensörü Anahtar Dağıtım Talebi [r123.1]
7	§ 5.3.7	Üye Ülke Otoritesi (MSA), Ek D'de tanımlanan anahtar dağıtım talebi (KDR) protokolünü kullanarak ERCA'dan hareket sensörü ana anahtarlarını talep etmelidir.	§6.5 Anahtar Sertifikası Talepleri ve Hareket Sensörü Anahtar Dağıtım Talebi [r123.3]
8	§ 5.3.8	Üye Ülke Otoritesi (MSA), Ek B'de tanımlanan dağıtım formatı uyarınca ERCA açık anahtarını kabul etmelidir.	§6.5 Anahtar Sertifikası Talepleri ve Hareket Sensörü Anahtar Dağıtım Talebi [r123.2]
9	§ 5.3.9	Üye Ülke Otoritesi (MSA), anahtar ve sertifika taşıma için Ek C'de tanımlanan fiziksel ortamı kullanmalıdır.	§6.5 Anahtar Sertifikası Talepleri ve Hareket Sensörü Anahtar Dağıtım Talebi [r123.4]
10	§ 5.3.10	Üye Ülke Otoritesi (MSA), ERCA'ya sertifika üretimi için sunulan Anahtar Tanımlayıcının (KID) ve anahtarların modulus (n) verisinin, Üye Ülke Sertifika Üretim Otoroitesi (MSCA) bağlamında benzersiz olmasını sağlamalıdır.	§6.5 Anahtar Sertifikası Talepleri ve Hareket Sensörü Anahtar Dağıtım Talebi [r123.5]
11	§ 5.3.11	Üye Ülke Otoritesi (MSA), süresi dolmuş anahtarların hiçbir amaçla kullanılmamasını sağlamalıdır. Üye ülke gizli anahtarı ya tekrar elde edilemeyecek biçimde yok edilmelidir, ya da kullanımı engellenecek biçimde saklanmalıdır.	§6.2.7 Türkiye Anahtarlarının Kullanımdan Kaldırılması [r116]
12	§ 5.3.12	Üye Ülke Otoritesi (MSA), bir cihaz RSA anahtarının gizliliğinin ve bütünlüğünün korunarak üretilmesini, taşınmasını ve cihaza yerleştirilmesini sağlamalıdır. Bu amaçla, Üye Ülke Otoritesi (MSA): a) Cihazın güvenlik sertifikasında zorunlu kılınan geçerli talimatların karşılanmasını sağlamalıdır, b) Hem üretimin hem de yüklemenin (eğer kart üzerinde değilse) fiziksel olarak güvenliği sağlanmış bir ortamda yapılmasını sağlamalıdır, c) Anahtar üretiminin cihazın güvenlik sertifikasında kapsanmadığı durumlarda, belirlenmiş ve uygun kriptografik anahtar üretim algoritmalarının kullanıldığından emin olmalıdır. Üretimle ilgili bu gerekliliklerin son ikisi, cihaz	§5.1.1 Kalite Kontrol – TR-CA/TR-CP Faaliyeti [r27] §7.1 Genel Durum - TR-CP / TR-CA, Hizmet Kuruluşları ve Takograf Cihazı Üreticileri [r124]'den [r126] §7.2 Donanım Anahtarı Üretimi

		anahtarlarını aşağıdaki donanımlardan biriyle üreterek karşılanabilir: a) FIPS 140-2 (veya FIPS 140-1) seviye 3 veya üstü [9] içeriğinde belirtilen gereklilikleri sağlamak üzere belgelendirilmiş; b) CEN Workshop Agreement 14167-2 [10] içeriğinde belirtilen gerekliliklerle uyumlu olduğuna dair belgelendirilmiş; c) ISO 15408'e [12] göre EAL4 veya üstü, ITSEC'e [13] göre seviye E3 veya üstü veya eşdeğer güvenlik kriterlerine uygunluğu temin edilmiş bir güvenilir sistem. Bu değerlemeler bir koruma profiline ya da güvenlik hedefine yönelik olmalıdır. d) Eşdeğer bir güvenlik seviyesi sağladığı gösterilmiş.	
13	§ 5.3.13	Üye Ülke Otoritesi (MSA), MSA Politikasının denetiminde üretilen, saklanan ve kullanılan gizli anahtarların gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamalıdır.	§3.4.1 Gizli Tutulması Gereken Bilgiler [r20] §6.2.1 Türkiye Anahtarları Üretimi §6.2.3 Türkiye Anahtarının Saklanması §6.4 Taşıma Anahtarları §7.2 Donanım Anahtarı Üretimi
14	§ 5.3.14	Üye Ülke Otoritesi (MSA), MSA Politikasının denetiminde üretilen, saklanan ve kullanılan gizli anahtarların yetkisiz kullanımını engellemelidir.	§6.2.3 Türkiye Anahtarının Saklanması §6.4 Taşıma Anahtarları §7.2 Donanım Anahtarı Üretimi §7.2.3 Donanım Gizli Anahtarının Korunması ve Saklanması - Kartlar
15	§ 5.3.15	Üye ülke gizli anahtarları, en az iki kişinin kontrolünü gerektiren bir anahtar kurtarma prosedürü kullanılarak yedeklenebilir.	§6.2.4 Türkiye Gizli Anahtarının Yedeklenmesi [r111]
16	§ 5.3.16	Gizli anahtarların taşınmasına dayanan anahtar sertifikalandırma taleplerine izin verilmez.	§6.5 Anahtar Sertifikası Talepleri ve Hareket Sensörü Anahtar Dağıtım Talebi [r123.6]

			§7.2.3 Donanım Gizli Anahtarının Korunması ve Saklanması - Kartlar [r143]
17	§ 5.3.17	Anahtar saklama kesinlikle yasaklanmıştır.	§6.2.5 Türkiye Gizli Anahtarının Emanette Saklamak [r112] §7.2.5 Donanım Gizli Anahtarının Emanet Edilmesi ve Arşivlenmesi [r147]
18	§ 5.3.18	Üye Ülke Otoritesi (MSA), hareket sensörü anahtarlarının yetkisiz kullanımını engellemelidir.	§6.3 Hareket Sensörleri Anahtarları [r120], [r122]
19	§ 5.3.19	Üye Ülke Otoritesi (MSA), hareket sensörü ana anahtarının (Km), hareket sensörü üreticilerinin amaçları doğrultusunda sadece hareket sensörü verilerinin şifrelenmesi için kullanılmasını sağlamalıdır. Şifrelenecek veriler ISO/IEC 16844-3 standardında [7] tanımlanmıştır.	Uygulanabilir Değil: §3.1.7 Hareket Sensörü Üreticilerinin Yükümlülükleri (kişiselleştirme organizasyonu olarak görev alan)
20	§ 5.3.20	Hareket sensörü ana anahtarı (Km), Üye Ülke Otoritesi'nin (MSA) güvenli ve kontrollü ortamını hiçbir zaman terk etmemelidir.	Uygulanabilir Değil: §3.1.7 Hareket Sensörü Üreticilerinin Yükümlülükleri (kişiselleştirme organizasyonu olarak görev alan)
21	§ 5.3.21	Üye Ülke Otoritesi (MSA), servis kartı hareket sensörü anahtarını (KmWC), bileşen kişiselleştiricisine (bu durumda, kart kişiselleştirme servisine), uygun biçimde güvenliği sağlanmış yöntemlerle, sadece servis kartlarına yerleştirilmesi amacıyla yönlendirmelidir.	§6.3 Hareket Sensörleri Anahtarları [r120]
22	§ 5.3.22	Üye Ülke Otoritesi (MSA), taşıt birimi (takograf cihazı) hareket sensörü anahtarını (KmVU), bileşen kişiselleştiricisine (bu durumda, taşıt birimi üreticisine), uygun biçimde güvenliği sağlanmış yöntemlerle, sadece taşıt birimlerine yerleştirilmesi amacıyla yönlendirmelidir.	Uygulanabilir Değil: §3.1.6 Takograf Cihazı Üreticilerinin Yükümlülükleri (kişiselleştirme organizasyonu olarak görev alan)
23	§ 5.3.23	Üye Ülke Otoritesi (MSA), hareket sensörü anahtar kopyalarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamalıdır.	§6.3 Hareket Sensörleri Anahtarları [r122]
24	§ 5.3.24	Üye Ülke Otoritesi (MSA), hareket sensörü anahtar kopyalarının aşağıdaki cihazlardan birinde saklanmasını sağlamalıdır. a) FIPS 140-2 (veya FIPS 140-1) seviye 3 veya üstü [9] içeriğinde belirtilen gereklilikleri sağlamak üzere belgelendirilmiş; b) ISO 15408'e [11] göre EAL4 veya üstü,	§6.3 Hareket Sensörleri Anahtarları [r122]

		ITSEC'e [12] göre seviye E3 veya üstü veya eşdeğer güvenlik kriterlerine uygunluğu temin edilmiş bir güvenilir sistem. Bu değerlemeler bir koruma profiline ya da güvenlik hedefine yönelik olmalıdır.	
25	§ 5.3.25	Üye Ülke Otoritesi (MSA), takograf cihazı ve takograf kartı donanımı açık anahtar sertifikalarını üretebilmek için farklı Üye Ülke Anahtar Çiftlerine sahip olmalıdır.	Uygulanabilir Değil:
26	§ 5.3.26	Üye Ülke Otoritesi (MSA), açık anahtarlı sertifikalandırma hizmeti donanımının erişilebilirliğini sağlamalıdır.	§6.2.1 Türkiye Anahtarları Üretimi [r106]
27	§ 5.3.27	Üye Ülke Otoritesi (MSA), Üye Ülke Gizli Anahtarlarını sadece aşağıdaki amaçlarla kullanmalıdır: a) Ek 1B İlave 11 Ortak Güvenlik Mekanizmaları [6] içeriğinde tanımlanmış ISO/IEC 9796-2 sayısal imza algoritmasını kullanarak Ek 1B cihaz anahtar sertifikalarını üretmek. b) Ek A'da tanımlandığı gibi, ERCA anahtar sertifikalandırma talebi üretmek. c) Eğer sertifika durum bilgisi sağlamak için bu yöntem kullanılıyorsa, Sertifika İptal Listeleri yayınlamak (bkz. 5.3.30).	§6.2 Türkiye Anahtarları [r100]
28	§ 5.3.28	Üye Ülke Otoritesi (MSA),cihaz sertifikalarını, Üye Ülke Gizli Anahtarlarını saklamak için kullanılan cihazda imzalamalıdır (bkz. 5.3.2).	§6 Kök Anahtarlar ve Taşıma Anahtarlarının Yönetimi: Avrupa Kök Anahtarı, Türkiye Anahtarları, Hareket Sensörü Anahtarları, Nakil Anahtarları – paragraf 9 §6.2.3 Türkiye Anahtarının Saklanması [r109]
29	§ 5.3.29	Üye Ülke Otoritesi (MSA), kendi bağlamı içinde, cihaz açık anahtarlarının Ek 1(B) [6]'de yer alan talimatlara uygun, benzersiz bir anahtar betimleyicisi ile tanımlanmasını sağlamalıdır.	§7.2 Donanım Anahtarı Üretimi [r136] §8.1.1 Takograf Kartları [r151]
30	§ 5.3.30	Anahtar üretimi ve sertifikalandırma aynı fiziksel güvenlikli ortamda yapılmadığı sürece, anahtar sertifikalandırma protokolü, sertifika taleplerinin bütünlüğü ve kaynağı hakkında, gizli anahtarı açığa çıkarmadan kanıt sağlamalıdır.	§8.1.1 Takograf Kartları [r151.1]
31	§ 5.3.31	Üye Ülke Otoritesi (MSA), sertifika durum bilgisinin erişilebilir olmasını sağlamalıdır.	§8.7 Donanım Sertifikası ve Bilgisinin Yayımlanması [r164.1] §8.9 Donanım Sertifikalarının

			İptali [r166]
32	§ 5.3.32	Bir takograf kartı sertifikasının geçerlilik süresi, ilgili takograf kartının geçerlilik süresiyle aynı olmalıdır.	§8.4 Donanım Sertifikalarının Geçerlilik Süresi [r160]
33	§ 5.3.33	Üye Ülke Otoritesi (MSA), geçerlilik süresi belirsiz sertifikaların takograf kartlarına yüklenmesini engellemelidir.	§8.4 Donanım Sertifikalarının Geçerlilik Süresi [r160]
34	§ 5.3.34	Üye Ülke Otoritesi (MSA), geçerlilik süresi belirsiz Üye Ülke sertifikalarının taşıt birimlerine yüklenmesine izin vermelidir.	Uygulanabilir Değil: §3.1.6 Takograf Cihazı Üreticilerinin Yükümlülükleri (kişiselleştirme organizasyonu olarak görev alan)
35	§ 5.3.35	Üye Ülke Otoritesi (MSA), kart üretim sürecinin bir aşamasında kart sahiplerinin kimliklerinin doğrulanmasını sağlamalıdır.	§5.1.2.1 Kullanıcı Uygulaması [r30]'dan [r33]'e §5.1.9 Kullanıcıya Kartın Teslimatı – TR-CP veya TR-CIA Faaliyeti [r70]
36	§ 5.3.36	Üye Ülke Otoritesi (MSA), herhangi bir Üye Ülke Otoritesi (MSA) anahtarının kaybının, çalınmasının veya potansiyel açığa çıkma durumunun gecikmeksizin ERCA'ya bildirilmesini sağlamalıdır.	§6.2.6 Türkiye Anahtarlarının Güvenliğinin Yitirilmesi [r113], [r114]
37	§ 5.3.37	Üye Ülke Otoritesi (MSA), ERCA'nın geri dönüş süresine bağımlı kalmayan felaket kurtarma mekanizmalarını oluşturmalıdır.	§6.2.1 Türkiye Anahtarları Üretimi [r106] §9.7 TR-CA/TR-CP İş Sürekliliği Planı [r215]
38	§ 5.3.38	Üye Ülke Otoritesi (MSA), dâhil olan tüm süreçler için bir risk değerlendirmesine dayanan bir bilgi güvenliği yönetim sistemi (BGYS) kurmalıdır.	§9.1 TR-CA ve TR-CP'nin Bilgi Güvenliği Yönetimi [r170]
39	§ 5.3.39	Üye Ülke Otoritesi (MSA), politikaların eğitim, klerans ve rolleri kapsadığını sağlamalıdır.	§9.3 TR-CA/TR-CP'nin Personel Güvenlik Kontrolleri
40	§ 5.3.40	Üye Ülke Otoritesi (MSA), sertifikalandırma işlemlerinin uygun kayıtlarının tutulmasını sağlamalıdır.	§9.6.1 TR-CIA Tarafından Kaydedilen Olayların Tipi [r205] §9.6.2 TR-CA/TR-CP Tarafından Kaydedilen Olayların Tipi [r206]
41	§ 5.3.41	Üye Ülke Otoritesi (MSA), Üye Ülke Sertifika Otoritesinin (MSCA) sona ermesiyle ilgili hükümlere Üye Ülke Otoritesi (MSA) Politikasında yer vermelidir.	§10 TR-CA veya TR-CP Hizmetlerine Son Verilmesi
42	§ 5.3.42	Üye Ülke Otoritesi (MSA) Politikası, değişim prosedürlerini içermelidir.	§12 Politika Değişim Prosedürleri

43	§ 5.3.43	Üye Ülke Otoritesi (MSA) denetimi bu bölümdeki gerekliliklerin sürdürülmesini sağlamalıdır.	§11.2 Denetleme Kapsamındaki Konular [r230]'den [r232]'ye
44	§ 5.3.44	Üye Ülke Otoritesi (MSA), onaylanmış politika tarafından kapsanan işlemlerin başlamasından sonraki 12 ay içinde ilk denetimi gerçekleştirmelidir. Bir denetimde herhangi bir uygunsuzluk delili bulunmazsa, bir sonraki denetim sonraki 24 ay içinde yapılabilir. Bir denetimde uygunsuzluk delili bulunursa, bir sonraki denetim sonraki 12 ay içinde yapılmalıdır.	§11.1 Uyumluluk Denetiminin Sıklığı [r229]
45	§ 5.3.45	Üye Ülke Otoritesi (MSA), 5.3.43'te belirtildiği gibi denetim sonuçlarını raporlamalıdır ve denetim raporunu İngilizce olarak ERCA'ya sunmalıdır.	§11.5 Sonuçların Bildirilmesi [r235.1]
46	§ 5.3.46	Denetim raporu, bir uygulama programı da içerecek biçimde, Üye Ülke Otoritesi (MSA) yükümlülüklerini yerine getirmek için gerekli olan düzeltici faaliyetleri tanımlamalıdır.	§11.5 Sonuçların Bildirilmesi [r235.1]