.TR Alan Adları için DNSSEC Uygulama Bildirimi (.TR DPS)

v1.0

.TR Ağ Bilgi Sistemi (TRABIS)

14-03-2023

İçindekiler

1. GİRİŞ **5**
1.1. Genel Bakış . . . 5
1.2. Belge Adı ve Kimlikleme . . . 5
1.3. Topluluk ve Uygulanabilirlik . . . 6
1.3.1. ".TR" Kayıt Otoritesi . . . 6
1.3.2. ".TR" Kayıt Kuruluşu . . . 6
1.3.3. Alan Adı Sahibi . . . 6
1.3.4. Sorumlu Kişi . . . 6
1.4. Beyanname Yönetimi . . . 7
1.4.1. Beyanname Yönetim Organizasyonu . . . 7
1.4.2. İletişim Bilgisi . . . 7
1.4.3. Beyanname Değişiklik Prosedürleri . . . 7

2. YAYINLAMA VE BARINDIRMA **7**
2.1. BARINDIRMA . . . 7
2.2. Açık Anahtarların Yayınlanması . . . 7

3. OPERASYONEL GEREKLİLİKLER **7**
3.1 Alan Adlarının Anlamı . . . 7
3.2 Alt Zone Yöneticisinin Tanımlanması ve Doğrulanması . . . 8
3.3 DS Kayıtlarının Girilmesi . . . 8
3.4 Kapalı Anahtarın Sahipliğini Kanıtlama Yöntemi . . . 8
3.5 DS Kaynak Kaydının Kaldırılması . . . 8

4. TESİS, YÖNETİM VE OPERASYONEL KONTROLLER **8**
4.1. Fiziksel Kontroller . . . 8
4.1.1. Tesis Konumu ve Yapımı . . . 8
4.1.2. Fiziksel Erişim . . . 8
4.1.3. Elektrik ve Klima Sistemi . . . 9
4.1.4. Suya Maruz Kalma . . . 9
4.1.5. Yangın Önleme ve Koruma . . . 9
4.1.6. Medya Depolama . . . 9
4.1.7. Atık Bertarafı . . . 9
4.1.8. Tesis Dışı Yedekleme . . . 9
4.2. Prosedürel Kontroller . . . 9
4.2.1. Güvenilir Roller . . . 9
4.2.2. Görev Başına Gerekli İnsan Sayısı . . . 10
4.2.3. Her Rol için Tanımlama ve Kimlik Doğrulama . . . 10
4.2.4. Rollerin Ayrılığını Gerektiren Görevler . . . 10
4.3. Personel Kontrolleri . . . 10
4.3.1 Eğitim Gereklilikleri . . . 10
4.4. Denetim Loglama Prosedürleri . . . 10
4.4.1. Kaydedilen Olayların Türleri . . . 10
4.4.2. Log İşleme Sıklığı . . . 10

4.4.3. Denetim Logları Bilgilerinin Saklanma Süresi 10
4.4.4. Denetim Loglarının Korunması 11
4.4.5. Denetim Logları Yedekleme Prosedürleri 11
4.4.6. Denetim Logları Toplama Sistemi 11
4.4.7. Güvenlik Açığı İncelemeleri 11
4.5. Güvenlik İhlali ve Felaketlerin Telafisi 11
4.5.1. Olay ve Güvenlik İhlalleriyle Başa Çıkma Prosedürleri . . 11
4.5.2. Bozuk Bilgi İşlem Kaynakları, Yazılım ve/veya Veriler . . . 11
4.5.3. Kapalı Anahtarı Ele Geçirme Prosedürleri 11
4.5.4. İş Sürekliliği ve BT Felaket Kurtarma Yeterlilikleri 12
4.6. Varlık Sonlandırma 12

5. TEKNİK GÜVENLİK KONTROLLERİ 12
5.1. Anahtar Çifti Üretimi ve Kurulumu 12
5.1.1. Anahtar Çifti Üretimi 12
5.1.2. Açık Anahtar İletimi 12
5.1.3. Kapalı Anahtar Parametrelerinin Oluşturulması ve Kalite Kontrolü 12
5.1.4. Anahtar Kullanım Amaçları 13
5.2. Kapalı Anahtar Koruması ve Kriptografik Modül Mühendisliği Kontrolleri 13
5.2.1. Kriptografik Modül Standartları ve Kontrolleri 13
5.2.2. Kapalı Anahtar (m-of-n) Çok Kişili Kontrol 13
5.2.3. Kapalı Anahtar Emaneti 13
5.2.4. Kapalı Anahtar Yedekleme 13
5.2.5. Şifreleme Modülünde Kapalı Anahtar Depolama 13
5.2.6. Kapalı Anahtar Arşivi 14
5.2.7. Bir Kriptografik Modüle veya Bir Modülden Kapalı Anahtar Aktarımı 14
5.2.8. Kapalı Anahtarı Etkinleştirme Yöntemi 14
5.2.9. Kapalı Anahtarı Devre Dışı Bırakma Yöntemi 14
5.2.10. Kapalı Anahtarı Yok Etme Yöntemi 14
5.3. Anahtar Çifti Yönetiminin Diğer Yönleri 14
5.3.1 Açık Anahtar Arşivi 14
5.3.2 Anahtar Kullanma Süresi 14
5.4. Aktivasyon Verileri 14
5.4.1. Aktivasyon Verilerinin Oluşturulması ve Kurulumu 14
5.4.2. Aktivasyon Veri Koruması 15
5.4.3. Aktivasyon Verilerinin Diğer Yönleri 15
5.5. Bilgisayar Güvenlik Kontrolleri 15
5.6. Ağ Güvenliği Kontrolleri 15
5.7. Zaman damgası 16
5.8. Yaşam Döngüsü Teknik Kontrolleri 16

6. Zone İmzalama 16
6.1. Anahtar Uzunlukları, Anahtar Türleri ve Algoritmalar 16

6.2. Kimlik Doğrulamalı Varlık Reddi 16
6.3. İmza Formatı 16
6.4. Anahtar Değişimi 16
6.5. İmza Ömrü ve Yeniden İmzalama Sıklığı 16
6.6. Kaynak Kayıtlarının Doğrulanması 17
6.7. Kaynak Kayıtları Geçerlilik Süresi 17

7. UYGUNLUK DENETİMİ 17
7.1. Varlık Uygunluk Denetiminin Sıklığı 17
7.2. Denetçinin Kimliği/Nitelikleri 17
7.3. Denetçinin Denetlenen Tarafla İlişkisi 17
7.4. Denetimin Kapsadığı Konular 17
7.5. Eksiklik Sonucu Yapılan İşlemler 18
7.6. Sonuçların İletilmesi 18

8. YASAL KONULAR 18

Kullanılan Terimler ve Kısaltmalar

- ***BTK*** *- Bilgi Teknolojileri ve İletişim Kurumu*
- ***DNS*** *- Alan adı Sistemi (Domain Name System)*
- ***DPS*** *- DNSSEC Uygulama Bildirimi (DNSSEC Practice Statement)*
- ***DNSSEC*** *- DNS Güvenlik Eklentileri (Domain Name System Security Extensions)*
- ***KSK*** *- Anahtar İmzalama Anahtarı (Key Signing Key)*
- ***ZSK*** *- Zone İmzalama Anahtarı (Zone Signing Key)*
- ***RR*** *- Kaynak Kaydı (Resource Record)*
- ***RRSET*** *- Kaynak Kayıt Kümesi (Resource Record Set)*
- ***DS*** *- Yetkili İmzalayan (Delegation Signer)*
- ***NSEC*** *- Bir Sonraki Güvenli Kayıt (Next Secure Record)*
- ***NSEC3*** *- Sıradaki Güvenli Kayıt Versiyon 3 (Next Secure Record Version 3)*
- ***NSEC3PARAM*** *- Sıradaki Güvenli Kayıt Versiyon 3 Parametreleri (Next Secure Record Version 3 Parameters)*
- ***TTL*** *- Geçerlilik Süresi (Time to Live)*
- ***DNSKEY*** *- Açık Anahtarı İçeren DNS Kaydı*
- ***RRSIG*** *- Kaynak Kayıt İmzası (Resource Record Signature)*
- ***IANA*** *- İnternet Tahsisli Sayılar Yetkilisi (Internet Assigned Numbers Authority)*
- ***API*** *- Uygulama Programlama Arabirimi (Application Programming Interface)*
- ***TRABIS*** *- ".TR" Ağ Bilgi Sistemi (".TR" Network Information System)*
- ***IP*** *- İnternet Protokolü (Internet Protocol)*
- ***Public Key*** *- Açık Anahtar*
- ***Private Key*** *- Kapalı Anahtar*
- ***Child Zone*** *- Alt Zone*

- ***Framework*** - *Çerçeve*
- ***Domain Name*** - *Alan Adı*
- ***Registry*** - *Kayıt Otoritesi*
- ***Registrar*** - *Kayıt Kuruluşu*
- ***Registrant*** - *Alan Adı Sahibi*
- ***Relying Party*** - *Sorumlu Kişi*
- ***NS*** - *Ad Sunucusu (Name Server)*
- ***SY*** - *Sistem Yöneticisi (System Administrator)*
- ***GG*** - *Güvenlik Görevlisi (Security Officer)*
- ***BT*** - *Bilgi Teknolojisi (Information Technology)*
- ***Key Rollover*** - *Anahtar Değişimi*
- ***Escrow*** - *Emanet*
- ***Passphrase*** - *Parola*
- ***IETF*** - *İnternet Mühendisliği Görev Grubu (Internet Engineering Task Force)*
- ***Authenticated Denial of Existence*** - *Kimlik Doğrulamalı Varlık Reddi*
- ***SOA*** - *Yetki Bölgesi (Start of Authority)*

1. GİRİŞ

".TR Alan Adları için DNSSEC Uygulama Bildirimi" adlı bu belge, TRABIS tarafından DNSSEC politika ve uygulamalarının kapsamını belirtmek amacıyla yazılmıştır. TRABİS, BTK tarafından yönetilmektedir. DNSSEC'nin operasyonel ve altyapı detayları bu belgede açıklanmıştır.

Bu belge oluşturulurken RFC 6841: DNSSEC Politikaları ve DPS için Bir Çerçeve metninden yararlanılmıştır.

1.1. Genel Bakış

".TR" alan adları kayıt yetkisi Nic.tr'den TRABİS'e devredilmiştir. Yetki devrinden sonra TRABIS tarafından DNS altyapısı için güçlü güvenlik mekanizmaları sağlamak amacıyla DNSSEC sistemi oluşturulmuştur. Zira şifreli imzalama, DNS sistemini dağıtmak için daha güvenli bir seçenektir. Kök ve ikinci seviye zone'lardan alan adlarına uzanan güven zinciri, DNS verilerinin kaynağını ve aktarım sırasında veya aracılar tarafından değiştirilmediğini doğrular.

1.2. Belge Adı ve Kimlikleme

".TR" Alan Adları için DNSSEC Uygulama Bildirimi (.TR DPS)

Versiyon: 1.0

Yayınlanma tarihi: 14-03-2023

1.3. Topluluk ve Uygulanabilirlik

Bu bölümde, ekosistemdeki paydaşlar detaylarıyla açıklanır.

1.3.1. ".TR" Kayıt Otoritesi

TRABIS, Türkiye'deki ".TR" alan adlarının kayıt otoritesidir. TRABIS, üst düzey alan adlarının yönetimi ve teknik işleyişinden sorumludur. TRABİS ayrıca com.tr, net.tr, gov.tr gibi ikinci seviye alan adları için de hizmet vermektedir.

DNSSEC kapsamında TRABİS;

- bir zone'daki RR'ları imzalamak için KSK ve ZSK'leri üretir,
- seçilen algoritmalara göre kriptografik anahtarları üretir,
- ".TR" ve altındaki zone'ları imzalar (bkz. Bölüm 3.1),
- gerekli olduğunda ZSK ve KSK'leri günceller,
- akredite kayıt kuruluşlarından DS kayıtlarını alır, kontrol eder ve bunları zone'larda yayınlar,
- WHOIS kayıtlarını günceller,
- DS kayıtlarını akredite irtibatlar vasıtasıyla IANA'ya gönderir.

1.3.2. ".TR" Kayıt Kuruluşu

Alan adı sahibi adına, bir alan adının tescilinden ve yönetiminden (ayrıca DNS kayıtlarından) kayıt kuruluşları sorumludur. Akredite kayıt kuruluşları bu işlemleri gerçekleştirmek için API aracılığıyla TRABİS sistemine ulaşır. DNSSEC kapsamında kayıt kuruluşlarının, alan adı sahibi müşterileri adına DS kayıtlarını almaları beklenir. Kayıt kuruluşları daha sonra bu kayıtları API yardımıyla TRABIS sistemine eklemelidir.

1.3.3. Alan Adı Sahibi

Alan adı sahibi, belirli bir süre için alan adının sahibi olan kişi ya da kurumdur. Bir alan adı sahibi alan adının düzgün bir biçimde imzalandığından emin olmalıdır. Bir alan adı sahibi veya sorumlusu, alan adının içeriğini koruyan sunucularında RFC 8624 belgesinde 3.1. başlığında yer alan tabloda "DNSSEC Validation" sütununda "MUST" ve "RECOMMENDED" olarak belirtilmiş ve yine aynı belgede 3.3. başlığında yer alan tabloda "DNSSEC Delegation" sütununda "MUST" ve "MAY" olarak belirtilmiş algoritmalara uygun DS kayıtları oluşturmaktan sorumludur. Daha sonra bu DS kayıtlarını hizmet alınan kayıt kuruluşuna bildirmeleri gerekir.

1.3.4. Sorumlu Kişi

Sorumlu kişiler alan adı sahibinin zone'larını yönetmekten sorumludur. Bu bir hizmet sağlayıcısı, kayıt kuruluşu ya da alan adı sahibinin kendisi olabilir.

1.4. Beyanname Yönetimi

1.4.1. Beyanname Yönetim Organizasyonu

TRABIS, BTK tarafından yönetilmektedir.

1.4.2. İletişim Bilgisi

Adres: Eskişehir Yolu 10.Km No:276 06530 Çankaya / Ankara - Türkiye

Telefon : +90 (312) 210 00 60 - +90 (312) 988 00 60

E-posta: destek@trabis.gov.tr

1.4.3. Beyanname Değişiklik Prosedürleri

".TR" Alan Adlari için DPS belgesi, BTK tarafından yıllık olarak veya ihtiyaç duyuldukça revize edilmektedir.

2. YAYINLAMA VE BARINDIRMA

2.1. BARINDIRMA

Barındırma TRABİS tarafından sağlanmaktadır. Bu DPS belgesi www.trabis.gov.tr adresinde bulunabilir. Belge salt-okunur erişim halinde sunulur. İngilizce ve Türkçe olarak hazırlanmıştır.

2.2. Açık Anahtarların Yayınlanması

".TR" zone'larınınn DS kayıtları IANA ile paylaşılır.

3. OPERASYONEL GEREKLİLİKLER

3.1 Alan Adlarının Anlamı

".TR" alan adının yapısı İNTERNET ALAN ADLARI YÖNETMELİĞİ (https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=14416&MevzuatTur=7&MevzuatTertip=5) metninin 6. maddesinde açıklanmıştır. 20 adet ikinci seviye zone bulunmaktadır. Bunlar `.com.tr`, `.net.tr`, `.biz.tr`, `.info.tr`, `.bbs.tr`, `.name.tr`, `.org.tr`, `.web.tr`, `.gen.tr`, `.av.tr`, `.tv.tr`, `.dr.tr`, `.k12.tr`, `tel.tr`, `.bel.tr` `.gov.tr`, `.edu.tr`, `.pol.tr`, `.tsk.tr` ve `.kep .tr`. ".TR" alan adı için kişi ya da kurumlar başvurabilir. `.dr.tr`, `.k12.tr`, `.av.tr`, `.bel.tr .gov.tr`, `.edu.tr`, `.pol.tr`, `. tsk.tr` ve `.kep.tr` belge kontrolü ile tahsis edilir. Zone'ların geri kalanı belgesiz tahsis edilir. Bu nedenle başvurularda "ilk gelen ilk alır" yaklaşımı geçerlidir. ".TR" için alan adı kaydına ilişkin hüküm ve koşullar trabis.gov.tr adresinde yayınlanmaktadır. Politika, BTK tarafından yayınlanmakta ve revize edilmektedir.

3.2 Alt Zone Yöneticisinin Tanımlanması ve Doğrulanması

Kayıt kuruluşları, alt zone yöneticisini tanımlamalı ve doğrulamalıdır. DNSSEC'i işlevsel hale getirmek için, bir kayıt kuruluşunun API aracılığıyla, DS kaydı göndermesi gerekir çünkü alan adlarını kayıt kuruluşları yönetir.

3.3 DS Kayıtlarının Girilmesi

Kayıt kuruluşları DS kayıtlarını TRABİS'e iletir. Alan adı sahibine ait zone'un DS kayıtları, kayıt kuruluşları tarafından ".TR" zone'una kaydedilir. Kayıt kuruluşları DS kayıtlarını girdiği sırada kayıtlar TRABIS sistemi tarafından alan adı sunucusundan kontrol edilir. Doğrulama sonucuna göre DS kayıtları kabul edilir veya edilmez. TRABIS sisteminde, bir alan adı için en fazla 3 farklı DS kaydı olabilir. Her bir DS kaydı iki farklı hash türü ile eklenebilir, bu sebeple bir alan adının en fazla 6 adet DS kaydı bulunabilir.

3.4 Kapalı Anahtarın Sahipliğini Kanıtlama Yöntemi

Alt zone'un kapalı anahtarlarından TRABİS sorumlu değildir.

3.5 DS Kaynak Kaydının Kaldırılması

DS kayıtları, kayıt kuruluşları tarafından kaldırılır. Acil durumlarda, kayıt otoritesi gerekli doğrulamaları yaptıktan sonra DS kayıtlarını güncelleyebilir veya kaldırabilir.

NS kayıtları değiştirildiğinde, öncelikle DS kayıtları kaldırılmalıdır. DS kayıtları kaldırıldıktan sonra NS kayıtları güncellenebilir.

4. TESİS, YÖNETİM VE OPERASYONEL KONTROLLER

4.1. Fiziksel Kontroller

4.1.1. Tesis Konumu ve Yapımı

TRABIS, çok katmanlı güvenlik tasarımı nedeniyle kritik düzeydeki varlık ve konumları için fiziksel güvenlik kriterlerini sağlayan iki operasyonel tesise sahiptir. Bu tesisler coğrafi olarak birbirine yakın değildir. Tesislere giriş ve erişim izlenmektedir. Tesislerde kesintisiz hizmet sağlayabilmek için gerekli tüm ekipmanlar mevcuttur.

4.1.2. Fiziksel Erişim

Fiziksel erişimin kısıtlanması çok katmanlı olarak tasarlanmıştır ve yalnızca ilgili rollere sahip yetkili personel ekipmana ve ofise erişebilir. Kimlik tanıtmanın birden çok yolu vardır ve her kişinin rolüyle ilgili belirli bir erişim türü vardır.

Tüm girişler kayit altina alinir, izlenir ve veritabanlarında saklanır. Herhangi bir ziyaretçinin TRABİS yönetimi tarafından tanımlanması ve yetkilendirilmesi gerekmektedir.

4.1.3. Elektrik ve Klima Sistemi

Bu tesislerde nem kontrolü, klima, yedek güç kaynağı ve diğer gerekli ekipmanlar bulunmakta ve bir afet durumunda işlevselliğini garanti altına almak için sürekli olarak kontrol edilmektedir.

4.1.4. Suya Maruz Kalma

Tesisleri güvenli ve emniyetli tutmak için su baskını algılama ve koruma mekanizmaları kurulmuştur.

4.1.5. Yangın Önleme ve Koruma

Tesislerde yangın ve duman dedektörleri bulunur ve düzenli kontroller ve denetimler yapılır. Yangın alarmları diğer alarmlardan ayırt edilebilir niteliktedir ve olası afet durumları için personele eğitim verilmiştir.

4.1.6. Medya Depolama

Diskler, CD'ler/DVD'ler, flash diskler gibi her türlü depolama araçları, diğer ek güvenlik katmanları ile güvenli bir kabinde tutulur. Ayrıca kabinetler yangın, su baskını vb. doğal afetlere karşı korumalıdır.

4.1.7. Atık Bertarafı

Atık belgelerin imha edilmesi ve fiziksel cihazların tekrar kullanılamayacak şekilde parçalanarak bertaraf edilmesi gerekmektedir.

4.1.8. Tesis Dışı Yedekleme

Loglar gibi kritik veriler düzenli aralıklarla tesis dışında da yedeklenir ve saklanır.

4.2. Prosedürel Kontroller

4.2.1. Güvenilir Roller

Güvenilir roller, operasyonel görevlere TRABIS ile resmi sözleşmeli olarak atanmıştır. Bu roller;

Sistem Yöneticisi - SY,

Güvenlik Görevlisi- GG.

Her rolün sorumlulukları biribirinden farklıdır ve hiçbir rol çakışması yoktur. KSK takımı ve ZSK takımı gerekli teknik süreçleri oluşturup yayınlamaktan sorumludur.

4.2.2. Görev Başına Gerekli İnsan Sayısı

Farklı rollerin işbirliğine olan ihtiyaca göre belirlenir.

4.2.3. Her Rol için Tanımlama ve Kimlik Doğrulama

Her role atanabilmek için DNS ve DNSSEC'le ilgili bilgi sahibi olma ön koşuldur.

4.2.4. Rollerin Ayrılığını Gerektiren Görevler

ZSK'de rolleri olan kişiler, KSK'de de aynı role sahip olabilir veya tam tersi olabilir. DNSSEC anahtar malzemelerinin üretimi, kullanımı ve imhası gibi rollerin görevleri ayrılmıştır.

4.3. Personel Kontrolleri

DPS'in "Personel Kontrolü" bölümü, operasyonların güvenliğini ve bütünlüğünü sağlamanın önemli bir parçasıdır. Kuruluş içinde güvenilir rollere sahip personelin işe alınması, eğitimi ve yönetimi için prosedürleri ve gereklilikleri ortaya koymaktadır. Bu roller, hassas bilgilere erişim ve alan adlarının ve DNS'nin yönetimi ile ilgili sorumlulukları içerir ve bu nedenle, bu pozisyonları elinde bulunduran kişilerin nitelikli, deneyimli ve sicilinin temiz olması çok önemlidir.

4.3.1 Eğitim Gereklilikleri

4.4. Denetim Loglama Prosedürleri

Loglama mekanizması, bölüm 4.4.1'de belirtildiği gibi denetim kayıtlarını alır ve prosedür otomatiktir.

4.4.1. Kaydedilen Olayların Türleri

Anahtar oluşturma, etkinleştirme, devretme ve oturum açma, yedekleme, güvenlikle ilgili olaylar gibi diğer operasyonel etkinlikler dahil olmak üzere anahtarlarla ilgili tüm işlemler günlüğe kaydedilir.

4.4.2. Log İşleme Sıklığı

TRABIS, herhangi bir güvenlik olayı için logları hem otomatik hem de manuel olarak inceler. Her bir olay, daha fazla araştırma ve operasyon için belgelenir. Denetim logları, dosyalardaki şüpheli işlemler için de incelenir.

4.4.3. Denetim Logları Bilgilerinin Saklanma Süresi

Kaydedilen tüm veriler 2 yıl boyunca yerinde saklanır ve 10 yıl boyunca tesis dışında arşivlenir.

4.4.4. Denetim Loglarının Korunması

Log dosyalarının değiştirilmemesi ve tahrif edilmemesini garanti altına almak için yalnızca yetkili kişiler log kayıtlarına erişebilir. Değişikliklerin araştırılmasını kolaylaştırmak için, arşivlerde dosyaların birleştirilmesi gibi bütünlük mekanizmaları da uygulanır.

4.4.5. Denetim Logları Yedekleme Prosedürleri

Denetim logları haftalık olarak yedeklenir. Yedeklemeler, yalnızca yetkili kişilerin erişebildiği uzak bir özel sunucuda tutulur.

4.4.6. Denetim Logları Toplama Sistemi

Denetim toplama sistemi SY'nin gözetiminde çalışan bir sistemdir. SY, hizmeti güncel tutmaktan ve yedekleme dosyalarının bütünlüğünü gözden geçirmekten sorumludur.

4.4.7. Güvenlik Açığı İncelemeleri

Bütün anomaliler iç denetimle ya da üçüncü taraflardan destek alınarak tespit edilebilir. Söz konusu durumda inceleme dahili olarak yapılır.

4.5. Güvenlik İhlali ve Felaketlerin Telafisi

4.5.1. Olay ve Güvenlik İhlalleriyle Başa Çıkma Prosedürleri

Güvenlikle ilgili, sisteme zarar verebilecek tüm sorunlar olay olarak tanımlanır. Operatörler veya denetçiler, TRABİS'in bilgi güvenliği politikasına dayalı olarak bir olay keşfettiklerinde, operasyon ve teknik ekip devreye girer. Olay, anahtarların tehlikede olduğu durum gibi kritik olarak sınıflandırılırsa, operasyonel ve teknik ekipler prosedürü yeniden başlatmak ve temiz bir geçiş yapmak için birlikte çalışır.

4.5.2. Bozuk Bilgi İşlem Kaynakları, Yazılım ve/veya Veriler

Sistemin donanım veya yazılım bileşenlerinde bir olay meydana gelmesi durumunda, yedek bileşenler kurtarılmalıdır. TRABİS'in bilgi güvenliği politikasında belirtildiği gibi, bu tür durumlar için her bileşenin bir yedeği olmalıdır. Yedekleme bileşeninin önce test ortamında test edilmesi ve ardından canlı ortama aktarılması gerekir.

4.5.3. Kapalı Anahtarı Ele Geçirme Prosedürleri

TRABIS, ZSK veya KSK güvenliğinin ihlal edilmesi ya da herhangi bir şüpheli durumda gerçekleştirilecek bir acil durum anahtar değişimi planlamıştır. TRABİS ayrıca olayı ilgili kurum ve kuruluşlara da bildirir.

4.5.4. İş Sürekliliği ve BT Felaket Kurtarma Yeterlilikleri

TRABİS, bilgi güvenliği politikasında felaket kurtarma planlarından bahsetmiştir. Donanımların bulunduğu ana tesis için herhangi bir felaket durumunda yedek olarak ikinci bir tesis bulunmakta ve tüm işlemler o tesisten devam ettirilebilmektedir. Ayrıca, ana tesiste her donanım bileşeninin yedekleri bulunur ve her bileşeni kullanmadan önce test etmek için bir test ortamı da mevcuttur.

4.6. Varlık Sonlandırma

TRABİS'in varlıklar için bir fesih ve devir planı vardır. Güvenli bir geçiş yolunun seçilip uygulandığından emin olmak için bu prosedürlerin her biri TRABİS'in desteği ve rehberliği ile yürütülebilir.

5. TEKNİK GÜVENLİK KONTROLLERİ

5.1. Anahtar Çifti Üretimi ve Kurulumu

5.1.1. Anahtar Çifti Üretimi

KSK ve ZSK'ler bir yazılım aracılığıyla oluşturulur. Bu yazılım, eğitimli ve yetkili bir sistem yöneticisi tarafından yapılandırılır. Bu yapılandırma esnasında sistem yöneticisi anahtar için kullanılacak algoritmayı, anahtar uzunluğu, değişim süreleri vb. belirler.

5.1.2. Açık Anahtar İletimi

Bir anahtar çiftinin açık bileşeni, gönderim sırasında üçüncu taraflarca değiştirilmesini önlemek için güvenli bir şekilde iletilmelidir. Anahtar çiftini iletmek ve doğrulamak için kabul edilebilir yöntemler arasında, bir DNSKEY kaydı olarak çevrimiçi teslimat, güvenli ve kimliği doğrulanmış bir depoda yayınlama ve anahtar seramonisine katılan tanıklara çevrimdışı dağıtılan kanıtlar yer alabilir. Anahtarın genel ya da açık bileşeni, imzalama sisteminden çıkarılabilir, yetkili kişiler tarafından doğrulanabilir ve özel olarak atanmış bir kişi tarafından yayınlanabilir. Açık anahtarın teslimi, tüm süreçlerin takip edilmesini ve herhangi bir anormalliğin belgelenmesini sağlamak için tanıkların katılımını da içerebilir.

5.1.3. Kapalı Anahtar Parametrelerinin Oluşturulması ve Kalite Kontrolü

Hem kaynak verimliliğini hem de güvenliği sağlamak için kapalı anahtar parametrelerinin (anahtarın boyutu ve diğer güvenlik parametreleri) kalitesi kontrol edilmelidir. Bu, RSA parametrelerinin önceliğinin test edilmesini, anahtar üretiminin teknolojik trendler bağlamında uygun parametrelerle üretildiğinin teyit edilmesini ve doğrulanmış donanım cihazları ve yetkili kişilerin katılımı kullanılarak anahtar parametrelerin doğrulanmasını içerebilir. Anahtar

oluşturma işlemi ayrıca sözde rastgele sayı üretimi ve anahtar parametre kalitesi için kontroller içerebilir.

5.1.4. Anahtar Kullanım Amaçları

Kapalı anahtarlar, DNSKEY kayıtlarını imzalamak için veya otomatik imzalama için kullanılır, yalnızca bu amaçlar için kullanılmalıdır. Ortaya çıkan herhangi bir kaynak kayıt imzasının geçerlilik süresi 21 günden fazla olmamalıdır. Bir felaket durumunda, sonraki anahtar imzalama işlemlerini yürütme yeteneği hakkında makul endişeler varsa, standart kaynak kayıt imzası sona erme süresi geçersiz kılınabilir.

Bazı durumlarda, ek kaynak kayıt imzası kayıtları geçerlilik süresi 180 günü geçmeyecek şekilde önceden oluşturulabilir. Bu kayıtlar, bir anahtar yönetim tesisi ve tesis dışı bir depolama tesisi kullanılarak korunabilir. Bunların kullanımı üst yönetimin onayını gerektirebilir. Diğer durumlarda, DNSSEC için üretilen anahtarlar başka bir amaçla veya imzalama sistemi dışında kullanılamaz.

5.2. Kapalı Anahtar Koruması ve Kriptografik Modül Mühendisliği Kontrolleri

TRABIS DNSSEC sisteminde softHSM kullanılmaktadır. Kapalı anahtarlar softHSM dışında herhangi bir yerde bulunmamakta, saklanmamaktadır. Tüm kriptografik işlemler güvenli sunucularda gerçekleştirilir.

5.2.1. Kriptografik Modül Standartları ve Kontrolleri

5.2'de bahsedildiği gibi, TRABIS softHSM kullanır ve imzalama işlemi, korumalı imzalayıcı sunucusunda gerçekleşir.

5.2.2. Kapalı Anahtar (m-of-n) Çok Kişili Kontrol

SY tek başına yetkili olmasına rağmen, SO ve SY genellikle kapalı anahtar işlemlerini birlikte gerçekleştirir.

5.2.3. Kapalı Anahtar Emaneti

Kapalı anahtarlar emanet edilmemektedir.

5.2.4. Kapalı Anahtar Yedekleme

Kapalı anahtarlar SoftHSM'de tutulur. SY ayrıca şifrelenmiş bir dosya sistemi yedeği alır ve onu uzak bir depolamaya güvenli bir şekilde aktarır.

5.2.5. Şifreleme Modülünde Kapalı Anahtar Depolama

Uygulanmamıştır.

5.2.6. Kapalı Anahtar Arşivi

Kullanılmayan kapalı anahtarlar, 5.2.4'te açıklanan yedekleme dışında arşivlenmez.

5.2.7. Bir Kriptografik Modüle veya Bir Modülden Kapalı Anahtar Aktarımı

KSK'ler ve ZSK'ler, Bölüm 5.1.1'de açıklandığı gibi bir yazılım aracılığıyla üretilir.

5.2.8. Kapalı Anahtarı Etkinleştirme Yöntemi

KSK'ler ve ZSK'lerin aktivasyonu, imzalamada kullanılan yazılım tarafından otomatik olarak yapılır.

5.2.9. Kapalı Anahtarı Devre Dışı Bırakma Yöntemi

KSK'lerin ve ZSK'lerin devre dışı bırakılması, imzalamada kullanılan yazılım tarafından otomatik olarak yapılır.

5.2.10. Kapalı Anahtarı Yok Etme Yöntemi

KSK'ler ve ZSK'lerin imhası, süresi dolduğunda yazılım tarafından otomatik olarak yapılır..

Silinen bir KSK/ZSK'ye ihtiyaç duyulursa, 5.2.4'te açıklandığı gibi yedeklenmiş konumdan erişilebilir.

5.3. Anahtar Çifti Yönetiminin Diğer Yönleri

5.3.1 Açık Anahtar Arşivi

Açık anahtarlar arşivlenir ve yedeklenir.

5.3.2 Anahtar Kullanma Süresi

Süresi dolan ZSK'ler yenileri ile değiştirilir ve süresi dolan ZSK bir daha kullanılmaz.

5.4. Aktivasyon Verileri

5.4.1. Aktivasyon Verilerinin Oluşturulması ve Kurulumu

Aktivasyon verileri, softHSM'de kullanılan belirteçleri başlatmak veya yeniden başlatmak için kullanılan parolalardan oluşur. Güvenlik görevlileri tarafından oluşturulur ve TRABIS çevrimdışı sisteminde saklanır. Bir yere transfer edilmesi gerekiyorsa çevrimiçi olarak iletilir.

5.4.2. Aktivasyon Veri Koruması

Aktivasyon verilerinin korunması, güvenlik görevlilerinin temel sorumluluğudur. Bu, aktivasyon verilerine erişmek için gereken kimlik bilgilerinin korunmasını ve koruduğu kapalı anahtarların kaybolmasına, çalınmasına, değiştirilmesine, yetkisiz ifşasına veya yetkisiz kullanımına karşı koruma sağlamak için gerektiğinde aktivasyon verilerinin devre dışı bırakılmasını içerir. Her güvenlik görevlisi, aktivasyon verilerinin güvende tutulmasını sağlamalıdır. Güvenliğin ihlal edildiğine dair şüpheli bir durum varsa, derhal iptal edilmeli ve değiştirilmelidir.

5.4.3. Aktivasyon Verilerinin Diğer Yönleri

Aktivasyon veri koruma prosedürleri, yetkisiz erişimi önlemek için fiziksel anahtarları korumak ve aktivasyon verilerini çevrimdışı tutmak içindir. Acil durumlarda aktivasyon verilerine erişim sadece güvenlik görevlilerine verilmektedir. Parolaların gizli tutulması kendi sorumluluğunda olup, yetkisiz kişilerin sisteme erişimini engellemek TRBİS'in sorumluluğundadır.

5.5. Bilgisayar Güvenlik Kontrolleri

Anahtar çifti oluşturma ve kurulum işlemleri, denetim ve izleme amaçları için kaydedilen ve zamanlanan etkinliklerle, güvenli sistemler ve prosedürler kullanan güvenilir kişiler tarafından gerçekleştirilmelidir. Açık anahtarlar bant içinde, TLS/SSL tarafından korunan bir havuz aracılığıyla veya doğrudan tanıklara teslim edilebilir. Anahtar parametreleri kalite ve öncelik açısından kontrol edilmelidir. Anahtarlar, imzalama sistemi içinde yalnızca amaçlarına uygun olarak kullanılmalıdır.

Zaman damgaları dakika seviyesinde doğru olmalı ve güvenilir kaynaklardan elde edilmelidir.

İmzalama sistemleri, iletişim ağlarından izole edilmeli ve güvenlik duvarlarıyla korunmalıdır, erişim yetkili kişilerle sınırlandırılmalı ve imza sistemi tarafından başlatılan tüm veri aktarımları sağlanmalıdır. Üretim sunucularına yalnızca geçerli bir iş nedeni olan kişiler tarafından erişilmeli ve genel kullanıcıların hesabı olmamalıdır. Bilgisayar sistemleri, fiziksel erişimin yetkili personelle sınırlı olduğu güvenli tesislerde barındırılmalı ve tüm erişim girişimleri günlüğe kaydedilmelidir.

5.6. Ağ Güvenliği Kontrolleri

Anahtar imzalama etkinlikleri için kullanılan imzalayıcı sistem ve üretim ağı, diğer bileşenlerden mantıksal olarak ayrılmalı ve güvenlik duvarları kullanılarak izinsiz girişlere karşı korunmalıdır. Üretim ağına erişim, tanımlanmış uygulama süreçleri ve farklı ağ bölümleri arasındaki iletişim ile sınırlı olabilir. Bu sistemler güvenlik duvarları kullanılarak yönetilebilir. Güvenlik duvarı sistemleri aracılığıyla yönlendirilen tüm iletişim günlüğe kaydedilmeli ve iletişim ağı üzerinden aktarılan tüm hassas bilgiler şifrelenmelidir. Bazı durumlarda, imzalayan sistem herhangi bir iletişim ağına bağlı olmayabilir ve TLS onaylı bir

web sunucusu aracılığıyla üretim ağıyla iletişim kurabilir. İmzalama, dağıtım ve doğrulama sistemleri arasında veri aktarımı yalnızca imzalama sistemi tarafından başlatılabilir ve uzak bir ana bilgisayar tarafından başlatılamaz.

Bilgi işlem modüllerinin dünya ile bağlantısının kesilmesi ve veri aktarımının disklerle manuel olarak yapılması gerekir.

5.7. Zaman damgası

Anahtar değişim seremoni süresi, elektronik ve kağıt tabanlı denetim günlük kayıtları ve DNSSEC imza başlangıç ve sona erme süreleri güvenilir bir zaman kaynağından alınmalı ve her anahtar törenden önce kontrol edilmeli ve bir sorun varsa düzeltilmelidir. Kullanılan süre dakika seviyesinde doğru olmalıdır ve NTP vb. bir servisten alınabilir. Zaman ayrıca sistem saatleri ile senkronize edilebilir ve denetim günlüklerinin zaman damgası ve kaynak kayıt imzası kayıtlarının geçerlilik süresinin ayarlanması için kullanılabilir.

5.8. Yaşam Döngüsü Teknik Kontrolleri

6. Zone İmzalama

6.1. Anahtar Uzunlukları, Anahtar Türleri ve Algoritmalar

TRABIS, ilgili zone'lari imzalamak için ZSK kullanır. TRABIS, IETF standartlaştırılmış algoritmalarından biri olan 'ECDSA-p-256' algoritmasını kullanmaktadır.

6.2. Kimlik Doğrulamalı Varlık Reddi

Kimlik doğrulamalı varlık reddi için TRABIS, RFC 5155 içinde incelenebilen 'NSEC3'ü kullanır.

6.3. İmza Formatı

TRABIS, RFC 6605 ile tanımlanan "ECDSAP256SHA256" ("ECDSA Curve P-256 with SHA-256") algoritmasını kullanarak imza oluşturur.

6.4. Anahtar Değişimi

ZSK yenilemesi 90 günde bir, KSK yenilemeleri ise yıllık veya ihtiyaca göre gerçekleştirilir.

6.5. İmza Ömrü ve Yeniden İmzalama Sıklığı

İmza geçerlilik süresi KSK için 2 ay, ZSK için ise 1 ay civarındadır. KSK ve ZSK için yeniden imzalama sıklıkları sırasıyla aylık ve haftalıktır.

6.6. Kaynak Kayıtlarının Doğrulanması

Kayıt Otoritesi, .tr zonunda yayınlanmadan önce tüm kaynak kayıtlarının protokol standartlarına uygun olduğunu doğrular.

6.7. Kaynak Kayıtları Geçerlilik Süresi

Her DNSSEC kaynak kaydı RFC 4034 için geçerlilik süresi saniye cinsinden aşağıdaki şekilde belirtilir:

Kaynak Kaydı Türü	Geçerlilik Süresi
DNSKEY	43200
DS	21600
NSEC3	3600 (en az SOA kadar)
RRSIG	İmzalanmış kaynak kayıtları ile aynı.

7. UYGUNLUK DENETİMİ

Yılın belirli bir zamanında, tüm süreçlerin ve birimlerin daha önce açıklanan kalite ve prosedüre uygun olarak çalıştığından emin olmak için hem iç hem de dış denetimler yapılır.

7.1. Varlık Uygunluk Denetiminin Sıklığı

TRABİS yılda bir kez düzenli olarak denetimler gerçekleştirmektedir. Özel bir durum olması durumunda planlanan süre dışında denetim yapılabilir. Örneğin, güvenlik olayları.

7.2. Denetçinin Kimliği/Nitelikleri

TRABIS, dahili güvenlik uzmanlarının yanı sıra bilgi güvenliği, DNSSEC ve şifreleme konularında yetkin olan 3. taraflarla işbirliği yapmaktadır.

7.3. Denetçinin Denetlenen Tarafla İlişkisi

Dış denetimler için bu 3. taraflar TRABİS yönetmeliğine uyarak işbirliği yaparlar. Bu 3. şahıslar bağımsızdır, niteliklidir ve TRABİS ile hiçbir ilişkisi yoktur.

7.4. Denetimin Kapsadığı Konular

Denetimler, TRABİS'in bilgi güvenliği politikasına göre yapılır ve denetim prosedürü başlamadan birkaç gün önce, arşiv logları vb. tüm gereklilikler denetçiler için hazırlanır.

7.5. Eksiklik Sonucu Yapılan İşlemler

Denetim prosedürü sırasında herhangi bir eksiklik fark edilirse, bunun belgelenmesi ve TRABİS'e sunulması gerekir. Daha sonra operasyon ekibi bir plan olarak bir çözüm yürütür ve birkaç gün içinde operasyon ekibi tarafından yönetim ekibinin gözetiminde uygulamaya geçilmelidir.

7.6. Sonuçların İletilmesi

TRABİS'in bilgi güvenliği politikasına göre denetim raporunun gizli olması gerekmektedir.

8. YASAL KONULAR

- Kişisel olarak tanımlanabilir tüm bilgiler KVKK'ya uygun olarak ele alınır.
- Bu DPS, kamuoyunu bilgilendirmek amacıyla yazılmıştır ve dağıtım sonuçlarından TRABİS sorumlu değildir.
- Alan Adı Sahibi ile Kayıt Kurumu tescil ettiren arasındaki mali ve yasal düzenlemeler TRABİS portalında yer almaktadır.
- Bu DPS, Türkiye Cumhuriyeti yasalarına tabi olacaktır.