GELİR İDARESİ BAŞKANLIĞI

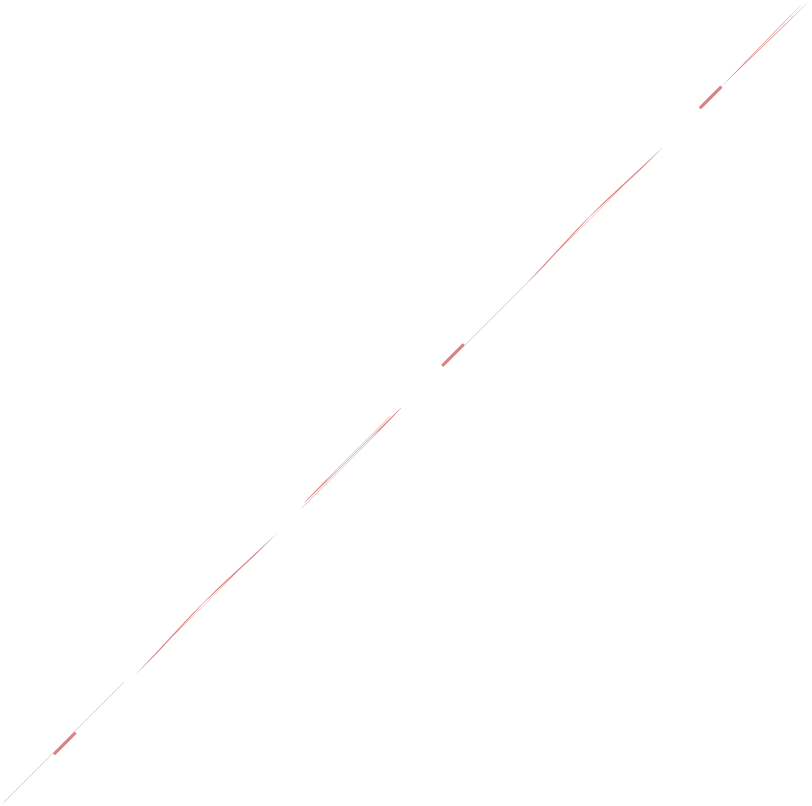
ELEKTRONİK DEFTER UYGULAMASI

SAKLAMA KILAVUZU

11 Mayıs 2020
ANKARA

GELİR İDARESİ BAŞKANLIĞI
Uygulama ve Veri Yönetimi Daire Başkanlığı (III)

Versiyon	Yayım Tarihi	Eklenen/Silinen/Değişen Bölüm	Açıklama
1.0	31.03.2020	--	Kılavuzun ilk yayım tarihi
1.1	11.05.2020	5. Bölüm Değişmiş, 7. Bölüm eklenmiştir.	Kılavuz güncellemesi



İçindekiler

1. GİRİŞ

Bilindiği üzere 6215 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanunun 14 üncü maddesi ile değiştirilen, 6762 sayılı Türk Ticaret Kanununun "Defter Tutma Mükellefiyeti" başlıklı 66 ncı maddesinin ikinci fıkrasında, söz konusu maddede geçen defterlerin (yevmiye defteri, defteri kebir, envanter defteri, karar ve işletme defteri) elektronik ortamda veya dosyalama suretiyle tutulabileceği ve bu defterlerin açılış ve kapanış onaylarının şekli ve esasları ile bu defterlerin nasıl tutulacağının Ticaret Bakanlığı ile Hazine ve Maliye Bakanlığı'nca çıkarılacak müşterek bir tebliğle belirleneceği hükme bağlanmıştır.

213 sayılı Vergi Usul Kanununun 5766 sayılı Kanunun 17 nci maddesi ile değişen mükerrer 242 nci maddesinin 2 numaralı fıkrası ile Hazine ve Maliye Bakanlığı; elektronik defter, kayıt ve belgelerin oluşturulması, kaydedilmesi, iletilmesi, muhafazası ve ibrazı ile defter ve belgelerin elektronik ortamda tutulması ve düzenlenmesi uygulamasına ilişkin usul ve esasları belirlemeye, elektronik ortamda tutulmasına ve düzenlenmesine izin verilen defter ve belgelerde yer alması gereken bilgileri internet de dâhil olmak üzere her türlü elektronik bilgi iletişim araç ve ortamında Hazine ve Maliye Bakanlığı'na veya Hazine ve Maliye Bakanlığı'nın gözetim ve denetimine tâbi olup, kuruluşu, faaliyetleri, çalışma ve denetim esasları Cumhurbaşkanlığı'nca çıkarılacak bir yönetmelikle belirlenecek olan özel hukuk tüzel kişiliğine haiz bir şirkete aktarma zorunluluğu getirmeye, bilgi aktarımında uyulacak format ve standartlar ile uygulamaya ilişkin usul ve esasları tespit etmeye, bu Kanun kapsamına giren işlemlerde elektronik imza kullanım usul ve esaslarını düzenlemeye ve denetlemeye yetkili kılınmıştır.

Ayrıca söz konusu fıkrada, Vergi Usul Kanunu ve diğer vergi kanunlarında defter, kayıt ve belgelere ilişkin olarak yer alan hükümlerin elektronik defter, kayıt ve belgeler için de geçerli olduğu; Maliye Bakanlığının, elektronik defter, belge ve kayıtlar için diğer defter, belge ve kayıtlara ilişkin usul ve esaslardan farklı usul ve esaslar belirlemeye yetkili olduğu hükme bağlanmıştır.

Vergi Usul Kanununun mükerrer 257 nci maddesinin birinci bendinde ise Hazine ve Maliye Bakanlığı'nın mükellef ve meslek grupları itibarıyla muhasebe usul ve esaslarını tespit etmeye, bu Kanuna göre tutulmakta olan defter ve belgeler ile bunlara ilaveten tutulmasını veya düzenlenmesini uygun gördüğü defter ve belgelerin mahiyet, şekil ve ihtiva etmesi zorunlu bilgileri belirlemeye, bunlarda değişiklik yapmaya; bedeli karşılığında basıp dağıtmaya veya üçüncü kişilere bastırıp dağıtmaya veya dağıttırmaya, bunların kayıtlarını tutturmaya bu defter ve belgelere tasdik, muhafaza ve ibraz zorunluluğu getirmeye veya kaldırmaya, bu Kanuna göre tutulacak defter ve düzenlenecek belgelerin tutulması ve düzenlenmesi zorunluluğunu kaldırmaya yetkili olduğu hükme bağlanmıştır. Söz konusu maddenin üçüncü bendinde, Hazine ve Maliye Bakanlığı'nın, tutulması ve düzenlenmesi zorunlu defter, kayıt ve belgelerin mikro film, mikro fiş veya elektronik bilgi ve kayıt araçlarıyla yapılması veya bu kayıt ortamlarında saklanması hususunda izin vermeye veya zorunluluk getirmeye, bu şekilde tutulacak defter ve kayıtların kopyalarının Hazine ve Maliye Bakanlığı'nda veya muhafaza etmekle görevlendireceği kurumlarda saklanması zorunluluğu getirmeye, bu konuda uygulama usul ve esaslarını belirlemeye yetkili olduğu hükme bağlanmıştır.

Diğer taraftan Vergi Usul Kanununun 175 inci maddesinin son fıkrasında Hazine ve Maliye Bakanlığı'nın, muhasebe kayıtlarını bilgisayar programları aracılığıyla izleyen mükellefler ile bu bilgisayar programlarını üreten gerçek ve tüzel kişilerce uyulması gereken kuralları ve bilgisayar programlarının içermesi gereken asgarî hususlar ile standartları ve uygulamaya ilişkin usul ve esasları belirlemeye yetkili olduğu hükmü yer almaktadır.

Ticari defterlere ilişkin usul ve esaslar bilindiği üzere Ticaret Bakanlığı ile Hazine ve Maliye Bakanlığı'nın müşterek olarak çıkarmış olduğu 19 Aralık 2012 tarih ve 28502 Sayılı Resmi gazetede yayımlanan "Ticari Defterlere İlişkin Tebliğ ile açıklanmıştır. Söz konusu Tebliğ'in 23. Maddesinde "Elektronik ortamda tutulacak defterler ile ilgili 13/12/2011 tarih ve 28141 sayılı Resmî Gazetede yayımlanan 1 Sıra Numaralı Elektronik Defter Genel Tebliği hükümleri uygulanır." hükmü bulunmaktadır.

13/12/2011 tarih 28141 sayılı Resmi Gazetede yayımlanan 1 Sıra Numaralı Elektronik Defter Genel Tebliğ ile standartları yayımlanan yevmiye defteri ve defteri kebirin elektronik ortamda oluşturulması imkanı getirilmiştir. Elektronik defterle ilgili Tebliğlere www.edefter.gov.tr resmi web sitesinden ulaşılmaktadır.

19/10/2019 tarih ve 30923 sayılı Resmi Gazetede yayımlanan 1 Sıra Numaralı Elektronik Defter Genel Tebliği'nde Değişiklik Yapılmasına Dair Tebliğ (Sıra No:3)'in "4.4. e-Defter Dosyaları, Berat Dosyaları ve Muhasebe Fişlerinin Muhafaza ve İbrazı" başlıklı bölümünün 4.4.1. maddesinin (e) fıkrasında;

"e-Defter dosyaları ile bunlara ilişkin berat dosyalarının ikincil kopyalarının, gizliliği ve güvenliği sağlanacak şekilde e-Defter saklama hizmeti yönünden teknik yeterliliğe sahip ve Başkanlıktan bu hususta izin alan özel entegratörlerin bilgi işlem sistemlerinde ya da Başkanlığın bilgi işlem sistemlerinde 1/1/2020 tarihinden itibaren asgari 10 yıl süre ile muhafaza edilmesi zorunludur. E-Defter ve beratların teknik yeterliğe sahip ve Başkanlıktan bu hususta saklama izni verilen özel entegratörlerin bilgi işlem sistemlerinde muhafaza usulü ile muhafaza edilmesi sürecinde e-Defter uygulamasına dâhil olan mükellefler ve özel entegratörler tarafından uyulması gereken genel, gizlilik ve güvenliğe ilişkin usul ve esaslar, Başkanlık tarafından hazırlanarak edefter.gov.tr adresinde yayımlanan "e-Defter Saklama Kılavuzu"nda açıklanır. e-Defter ve berat dosyalarına ait ikincil kopyalarının bu fıkra uyarınca muhafazası için gerekli yükleme işlemlerinde bu Tebliğin (4.3.4) numaralı fıkrasında belirtilen süreler dikkate alınır."

hükmüne yer verilmiştir.

Hazırlanan bu doküman ile e-Defter uygulaması kapsamında saklama hizmeti vermek isteyen özel entegratör kuruluşların sahip olması gereken altyapı, sistem, uluslararası sertifika vb. konular açıklanmaktadır.

2. AMAÇ

Bu kılavuz vasıtasıyla, 19/10/2019 tarih ve 30923 sayılı Resmi Gazetede yayımlanan 1 Sıra Numaralı Elektronik Defter Genel Tebliği'nde Değişiklik Yapılmasına Dair Tebliğ (Sıra No:3) ile, e-Defter saklayıcı kuruluşlar vasıtasıyla; mükelleflerin e-Defter uygulaması kapsamında oluşturdukları e-Defterler ile Berat dosyalarının gizliliği ve kriptolu olarak güvenliği sağlanmış bir şekilde ikincil kopyalarının saklanması, Gelir İdaresi Başkanlığı tarafından ihtiyaç duyulması halinde uzaktan erişimine imkan verilmesi, amaçlanmaktadır.

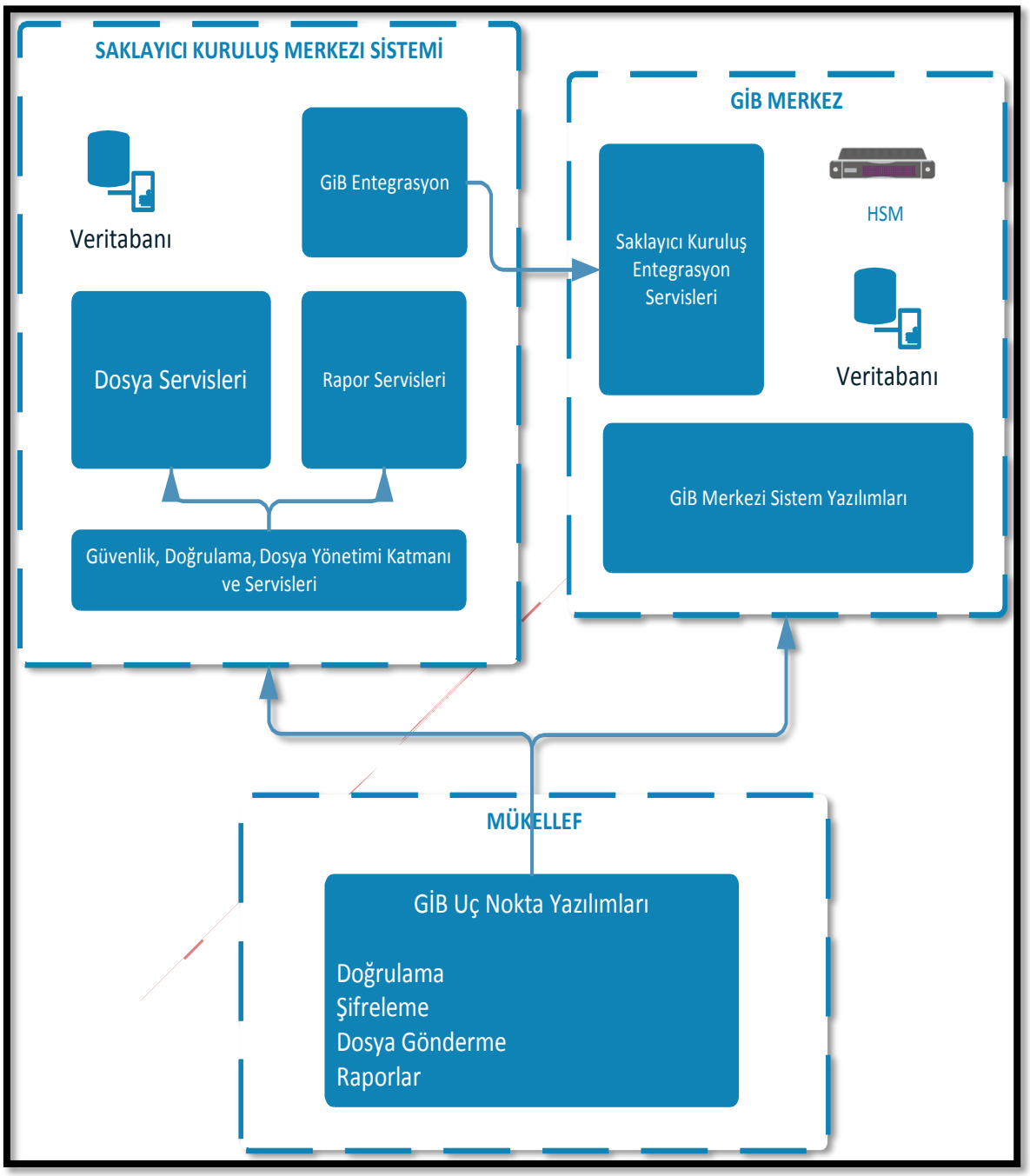
3. TANIMLAR VE KISALTMALAR

Tanım	Açıklama
Kurum, İdare, GİB, Başkanlık	Gelir İdaresi Başkanlığı
Firma, Saklayıcı Kuruluş, özel entegratör	Kılavuz kapsamındaki isterlere haiz, gerekli sorumlulukları yerine getiren ve mükelleflere hizmet sunmaya istekli kuruluşlar
Saklayıcı Kuruluş Merkezi Sistem Yazılımları	Saklayıcı Kuruluşların merkezi sistemlerinde çalışan, GİB Uç Nokta Yazılımları ve GİB Merkezi Sistem Yazılımları ile haberleşen, kılavuzdaki isterleri yerine getiren merkezi sistem yazılımları
GİB Merkezi Sistem Yazılımları	GİB merkezi sisteminde çalışan; Anahtar Yönetimi, Doğrulama Sistemi, Uç Nokta Yazılımları Yönetimi, Şifreleme Altyapısı, Güvenli Kanal gibi Sistemin merkezi ve yönetimsel fonksiyonlarını üstlenen merkezi sistem yazılımları
GİB Uç Nokta Yazılımları	Mükellef ortamlarında çalışan, GİB ve Saklayıcı Kuruluş bağlantılarını yöneten, dosya şifreleme, görüntüleme ve gönderme gibi foknsiyonları üstlenen uç nokta yazılımları.
Saklayıcı Kuruluş Özel Dosya Depolama Birimi	Saklayıcı Kuruluşa ait fiziksel ve güvenli ortamlarda; mükelleflere ait şifreli dosyaların iletiminden itibaren 10 yıl boyunca saklanacağı, ikincil kopyalarının fiziksel olarak farklı bir lokasyonda yedeklendiği özel dosya saklama birimidir.

4. SİSTEM MİMARİSİ, AKIŞLAR ve GÜVENLİK ALTYAPISI

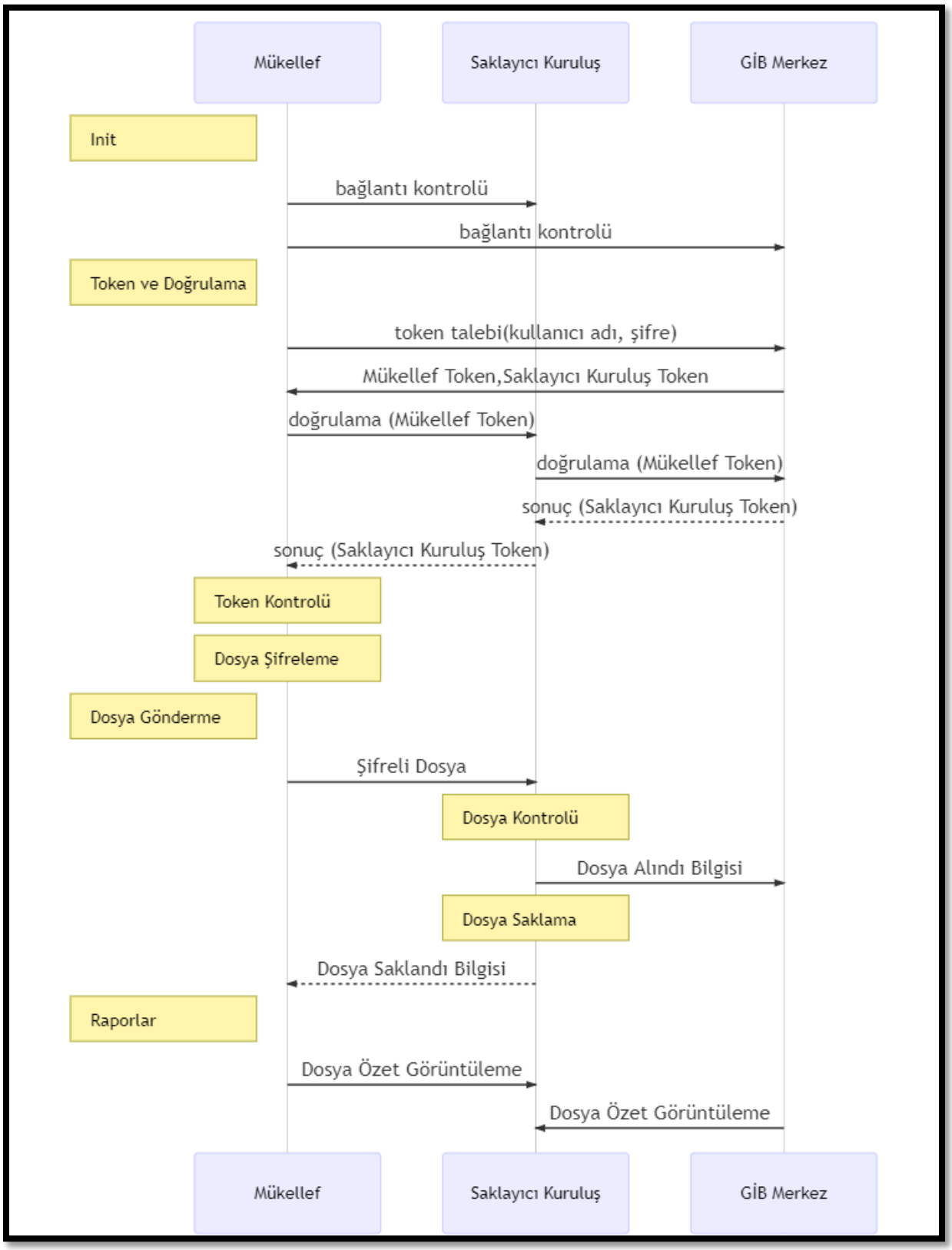
4.1 SİSTEM MİMARİSİ

Sistem mimarisi aşağıdaki şekildedir.



4.2 TEKNİK AKIŞLAR

Genel işlem akışı aşağıdaki şekilde olacaktır.



Dosyaların Saklayıcı Kuruluş Merkezi Sistemine Alınması ve Depolanması:

- Mükellef, Saklayıcı Kuruluş seçimini kurulum esnasında Portal üzerinden yapacaktır.

- Mükellefin seçimini yaptığı saklayıcı kuruluş merkezi sistemi erişim bilgileri GİB Uç Nokta Yazılımları tarafından otomatik olarak yönetilecektir.

- Dosyaların Saklayıcı Kuruluş Merkezi Sistemine gönderimi, GİB Uç Nokta Yazılımları tarafından GİB konfigürasyonuna göre her ayın belirli günlerinde olabilecektir. GİB, talep edilmesi halinde Saklayıcı Kuruluşlara bu konfigürasyonlarla ilgili bilgilendirme yapabilecektir.

- Mükellefe ait dosyalar, uç noktada GİB tarafından sağlanan yazılımlar ile, GİB anahtarları kullanılarak şifrelenecektir.

- GİB Uç Nokta Yazılımları, dosyaları göndermeden önce GİB Merkezi Sistemi üzerinden Saklayıcı Kuruluşa ait bir adet token (Saklayıcı Kuruluş Token)ve mükellefe/muhasebeciye ait kullanıcı bilgileri ile bir adet token(Mükellef Token) alacaktır.

- GİB Uç Nokta Yazılımları, GİB Merkezi Sistemi üzerinden aldığı Mükellef Token değeri ile Saklayıcı Kuruluş Merkezi Sistemi Yazılımlarına güvenli bağlantı kurma talebi iletecektir.

- Saklayıcı Kuruluş Merkezi Sistemi Yazılımları, GİB Uç Nokta Yazılımlarından gelen Mükellef Token değerini GİB Merkezi Sistemi Servislerine doğrulatıp sonuç bilgisini ve sonuç bilgisi ile gelen Saklayıcı Kuruluş Token bilgisini GİB Uç Nokta Yazılımlarına iletecektir.

- GİB Uç Nokta Yazılımları, Saklayıcı Kuruluş Merkezi Sisteminden gelen Saklayıcı Kuruluş Token bilgisi ile GİB Merkezi Sistemi üzerinden aldığı Saklayıcı Kuruluş Token değerini de ayrıca karşılaştıracaktır.

- Mükellef, GİB ve Saklayıcı Kuruluş arasındaki bu karşılıklı Doğrulama adımları başarılı olduktan sonra Dosyalar, güvenli bir kanal üzerinden şifreli olarak Saklayıcı Kuruluş Merkezi Sistemine aktarılacaktır.

- Saklayıcı Kuruluş Merkezi Sisteminde, GİB Uç Nokta Yazılımları tarafından gönderilen dosyaları karşıladığı noktada, OBJECT STORAGE depolama sistemi ve S3 (Simple Storage Service) depolama protokol desteği olacaktır. (Dosya aktarımı ve depolanmasında kullanılacaktır.)

- Saklayıcı Kuruluş Merkezi Sistemi, uç noktadan gelen dosyaları Saklayıcı Kuruluş Özel Dosya Depolama Birimine aktaracaktır.

- Şifreli dosyaların yedekleri ayrı bir fiziksel lokasyonda saklanmalıdır. Yedek dosyaların bu ikinci lokasyona iletilmesi anlık olarak yapılmalıdır. (FKM/DRC)

- Saklayıcı Kuruluş Merkezi Sistem Yazılımları, Saklayıcı Kuruluş Özel Dosya Depolama Birimine aldığı her bir şifreli Mükellef dosyası için, dosyayı aldığını bildirmek amaçlı olarak, aşağıdaki bilgileri GİB Merkezi Sistem Servislerine iletecektir.

GİB'e İletilecek Özet Bilgiler:

- Saklama Protokol Versiyonu
- Şifreleme Anahtar Verisyonu
- Mükellef Bilgileri ve/veya Muhasebeci Bilgileri
- Dosya İsmi
- Dosya Oluşturulma Tarihi
- Dosya Alınma Tarihi
- Dosya Boyutu
- Dosya Özet Değeri

- Saklayıcı Kuruluş Merkezi Sistemi ve GİB Merkezi Sistemi arasındaki iletişim, IPSec ve TLS 1.2 ve üzeri güvenli protokoller kullanılarak yürütülecektir.

- GİB Merkezi Sistem Servisleri, dosyalara ait bilgileri kendi sistemine aldıktan sonra her bir dosya için tekil bir ID(Dosya GİB Tekil Numarası) üretir ve bu değeri Saklayıcı Kuruluş Merkezi Sistem Yazılımlarına döner.

- Saklayıcı Kuruluş Merkezi Sistem Yazılımları, GİB Merkezi Sistem Servislerine dosyayı aldığı bilgisini başarılı şekilde iletene kadar her gün 5 defa deneme yapar.

- Saklayıcı Kuruluş Merkezi Sistem Yazılımları, GİB Merkezi Sistem Servislerine dosyayı aldığı bilgisini başarılı bir şekilde bildirdikten sonra, Dosya GİB Tekil Numarası ile Saklayıcı Kuruluş Özel Dosya Depolama Biriminde yer alan dosyayı eşleştirecektir.

- Servislere ait parametre ve format dokümanı, GİB tarafından Saklayıcı Kuruluş başvurusu onaylanan firmalara verilecektir. (Tüm Saklayıcı Kuruluşlardan servis input ve output formatlarının GİB tarafından belirlendiği gibi ve aynı olması istenecektir.)

Saklanan Dosyaların Özet Bilgilerinin Mükellef Tarafından Saklayıcı Kuruluş Merkezi Sisteminde Görüntülenmesi

- Saklayıcı Kuruluş Merkezi Sistem Yazılımları, e-Belge Özet Bilgilerini ve dosyalara ait Dosya GİB Tekil Numarası bilgisini, GİB Uç Nokta Yazılımları tarafından talep edildikçe HTTPS protokolü ile bir servis aracılığı ile iletilecektir.

- GİB Uç Nokta Yazılımları, mükelleflere saklanan dosyaların statülerini görebilecekleri bir arayüz sunacaktır. Bu arayüzde aşağıdaki bigiler yer almaktadır:

  - Saklama Protokol Versiyonu
  - Şifreleme Anahtar Verisyonu
  - Mükellef Bilgileri ve/veya Muhasebeci Bilgileri
  - Dosya İsmi
  - Dosya Oluşturulma Tarihi
  - Dosya Saklama Tarihi
  - Dosya Boyutu
  - Dosya Özet Değeri
  - Dosya GİB Tekil Numarası
  - Dosya Şifreleme Bilgisi (Evet/Hayır)
  - Dosya Saklayıcı Kuruluş Alma Bilgisi (Evet/Hayır)

- Dosya Saklandı Bilgisinin GİB'e Bildirimi(Evet/Hayır)

- Servislere ait parametre ve format dokümanı, GİB tarafından Saklayıcı Kuruluş başvurusu onaylanan firmalara verilecektir. (Tüm Saklayıcı Kuruluşlardan servis input ve output formatlarının GİB tarafından belirlendiği gibi ve aynı olması istenecektir.)

Saklanan Dosyaların GİB Merkezi Sistemine İletilmesi

Dosya Sorgulama

- Saklayıcı Kuruluş Merkezi Sistemleri, GİB anahtarları ile şifreli olarak depolanan dosyalara ait özet bilgileri bir servis ile, GİB Merkezi Sistemi Yazılımlarına vermelidirler. Bu servisin özellikleri aşağıdaki şekilde olmalıdır:

  - Serviste paging(sayfa sayfa veri getirme) mekanizması bulunmalıdır.
  - Serviste search(mükellef vb. kısıtlarla veri getirme) mekanizması bulunmalıdır.
  - Serviste login mekanizması bulunmalıdır.
  - Servis iletişim protokolü olarak HTTPS, TLS 1.2 ve üzeri desteklemelidir.
  - Servisin döneceği veriler aşağıdaki şekildedir:
    - Saklama Protokol Versiyonu
    - Şifreleme Anahtar Verisyonu
    - Mükellef Bilgileri ve/veya Muhasebeci Bilgileri
    - Dosya İsmi
    - Dosya Oluşturulma Tarihi
    - Dosya Saklama Tarihi
    - Dosya Boyutu
    - Dosya Özet Değeri
    - Dosya GİB Tekil Numarası
    - Dosya Şifreleme Bilgisi (Evet/Hayır)
    - Dosya Saklayıcı Kuruluş Alma Bilgisi (Evet/Hayır)
    - Dosya Saklandı Bilgisinin GİB'e Bildirimi(Evet/Hayır)
    - Session Bazlı Dosya Linki

  - Görüntülenen şifreli dosyalardan biri veya bir kaçı indirilmek istendiğinde, Session Bazlı Dosya Linkine tıklanımlası yeterli olacak.
  - Bu şifreli dosya özetlerinin görüntülenme ve indirilme erişimi sadece GİB Merkezi Sistemine açık olacak.

Dosya İletimi

- Saklayıcı Kuruluş Merkezi Sistem Yazılımları, GİB Merkezi Sistemi Yazılımları tarafından talep edilen dosyaları iletecek şekilde tasarlanacaktır.

- Saklayıcı Kuruluş Merkezi Sistemi, GİB Merkezi Sisteminin talep ettiği Dosya GİB Tekil Numarası'na ait dosyayı GİB Merkezi Sistemine anlık olarak iletecektir.

- GİB Merkezi Sistemi tekli veya çoklu dosya talebinde bulunabilecektir. Bu talep bir servis aracılı ile Saklayıcı Kuruluş Merkezi Sistem Yazılımlarına iletilecektir.

- Saklayıcı Kuruluş Merkezi Sistem Yazılımları, kendisine gelen dosya taleplerine cevap olarak ilgili dosyaları, GİB Merkezi Sistemine S3 protokolü ile iletecektir.

- Servislere ait parametre ve format dokümanı, GİB tarafından Saklayıcı Kuruluş başvurusu onaylanan firmalara verilecektir. (Tüm Saklayıcı Kuruluşlardan servis input ve output formatlarının GİB tarafından belirlendiği gibi ve aynı olması istenecektir.)

4.3 GÜVENLİK ALTYAPISI

4.3.1. Doğrulama

- **Saklayıcı Kuruluş Doğrulanması;**
    - GİB Uç Nokta Yazılımları; Saklayıcı Kuruluş doğrulamasını SSL sertifikası, IP bilgisi, Token ile yapar. Hangi saklayıcı kuruluş ile iletişime geçeceğini, mükellefin tercihi doğrultusunda GİB Merkezi sisteminden güvenli ve şifreli bir kanal üzerinden alır. GİB Uç Nokta Yazılımları, dosyaları göndermeden önce GİB Merkezi Sistemi üzerinden Saklayıcı Kuruluşa ait bir adet token (Saklayıcı Kuruluş Token) ve mükellefe/muhasebeciye ait kullanıcı bilgileri ile bir adet token(Mükellef Token) alacaktır. Bu Saklayıcı Kuruluş Token değeri Saklayıcı Kuruluşun Uç nokta tarafından doğrulanmasında kullanılacaktır.
      Her bir servis için ApiKey ve ApiPass doğrulaması yapılır. Tüm iletişim HTTPS, TLS 1.2 ve üzeridir.

    - GİB Merkezi Sistemi; Her bir Saklayıcı Kuruluş için IPSec tanımı yapılır. SSL sertifikası doğrulanır. Ayrıca her bir servis için ApiKey ve ApiPass doğrulaması yapılır. Tüm iletişim HTTPS, TLS 1.2 ve üzeridir.

- **GİB Uç Nokta Yazılımları ve Mükellef Doğrulaması**
    - GİB Uç Nokta Yazılımları, dosyaları göndermeden önce GİB Merkezi Sistemi üzerinden Saklayıcı Kuruluşa ait bir adet token (Saklayıcı Kuruluş Token)ve mükellefe/muhasebeciye ait kullanıcı bilgileri ile bir adet token(Mükellef Token) alacaktır. Bu Mükellef Token değeri Saklayıcı Kuruluşun Uç noktayı/Mükellefi doğrulamasında kullanılacaktır.
    - Her bir servis için ApiKey ve ApiPass doğrulaması yapılır. Tüm iletişim HTTPS, TLS 1.2 ve üzeridir.

- **GİB Merkezi Sistem Doğrulaması**
    - Saklayıcı Kuruluş tarafından IPSec ve Sertifika doğrulaması yapılır. Her bir servis için ApiKey ve ApiPass doğrulaması yapılır. Tüm iletişim HTTPS, TLS 1.2 ve üzeridir.
    - GİB Uç Nokta Yazılımları tarafından Sertifika doğrulaması yapılır. Tüm iletişim HTTPS, TLS 1.2 ve üzeridir.

4.3.2. Güvenli Kanal

- Mükellef, Saklayıcı Kuruluş, GİB arasındaki Tüm iletişim HTTPS, TLS 1.2 ve üzeridir.
- Tokenizasyon altyapısı ile her bir session için GİB Merkesi Sisteminde HSM cihazları üzerinde üretilen Token değerleri ile anlık olarak güvenli kanal oluşturulur.
- Oluşturulan kanallar mükellef ve session bazlı olarak tekildir.
- Güvenli kanalda Tokenizasyon kontrolleri, count ve zaman bazlıdır. Bu sayede her bir token belirli bir süre ve tek bir adet kullanılabilir

4.3.2.1.Veri Bütünlüğü

- Dosya ve veri transferi esnasında gönderici nokta ile alıcı nokta arasıdan veri bütünlüğünü kontrol etmek için hash mekanizması kullanılmaktadır. Dosyalar ve veriler gönderilmeden önce tuzlama yapılarak hash değerleri hesaplanıp, bu değer ile birlikte alıcıya iletilir. Alıcı Dosyayı ve veriyi aldığında bu kontolü yapar ve sonra sistemine kabül eder.
- Saklayıcı Kuruluş Merkezi Sistemi, GİB Uç Nokta Yazılımlarından gelen dosyalar için bu kontrolleri yapacaktır.
- Saklayıcı Kuruluş Merkezi Sistemi, GİB Merkezi Sistemine dosya gönderirken bu hesaplamaları yapacaktır.

4.3.2.2. Anahtar Yönetimi ve Şifreleme

GİB Merkezi Sistem Yazılımları, HSM cihazlarını kullanarak, Mükellef bazlı olarak GİB Uç Nokta Yazılımları için, özel anahtar ve sertifikalar üretmektedir.

Bu anahtarlar, Sistem altyapısı, Tokenizasyon, güvenli kanal oluşturma ve veri şifreleme adımlarında kullanılmaktadır.

Saklayıcı Kuruluş tarafından bilinmesi ve uygulanması gereken maddeler aşağıda sıralanmıştır:

- Tokenizasyon altyapısında AES algoritması kullanılmaktadır.
- Saklayıcı Kuruluş Token Değeri; Saklayıcı Kuruluş ID değeri, zaman bilgisi ve rasgele sayı üçlüsünden oluşan bir özelleştirme ile GİB Merkezi Sistemindeki Master AES anahtardan türetilen benzersiz bir anahtar ile şifreli veridir.
- Mükellef Token Değeri; Mükellef ID değeri, zaman bilgisi ve rasgele sayı üçlüsünden oluşan bir özelleştirme ile GİB Merkezi Sistemindeki Master AES anahtardan türetilen benzersiz bir anahtar ile şifreli veridir.
- GİB Uç Nokta Yazılımları, dosyaları GİB e ait Public anahtar ile(GİB Public KEY) şifrelemektedir.
- Dosyalar, yalnızca GİB tarafından çözülebilecek şekilde şifrelenmektedir.
- Dosyalar, Saklayıcı Kuruluşa şifreli olarak iletilmekte ve şifreli bir şekilde saklanmaktadır.
- Dosyaların şifrelendiği Public anahtarın eşleniği olan Private anahtar(GİB Private KEY) GİB Merkezi Sisteminde HSM cihazları içerisinde bulunmaktadır.
- GİB Master AES anahtarı belirli süreler ile değişmektedir.
- GİB Asimetrik Anahtar Çifti belirli süreler ile değişmektedir.

5. SAKLAMA HİZMETİ

Saklayıcı kuruluş hizmeti, saklama hizmeti kapsamında mükelleflerin yükleme yapabilmesi için, kullanımı ve kurulumu kolay ekranlarda, yükleme sırasında meydana gelebilecek kesilmeleri gözeterek sağlamalıdır. Ayrıca mükellef e-Fatura özel entegratörü ile çalışabileceği gözetilerek, aynı işlemi bir servis ile özel entegratörlere de sunacaktır. Bu durumda sisteme yüklenen bir e-Defterin hangi özel entegratör tarafından yüklendiği bilgisinin de Saklayıcı Kuruluş tarafından şüpheye yer bırakmayacak şekilde sağlanması gerekmektedir.

Mükelleflerin e-Defter boyutları çok büyük ya da çok küçük olabilir. Saklayıcı kuruluş mükelleflere ait e-Defter kayıtlarının şifreli olarak tutulmasını sağlayacak olan altyapıyı kendi bünyesinde sağlamalı, felaket kurtarma gibi her türlü yedekleme ve kurtarma önlemini alması beklenmektedir.

Bu kapsamda saklayıcı kurulusun sahip olması gereken teknik altyapı kriterleri aşağı belirtilmiştir.

5.1 Proje kapsamında saklayıcı kuruluşların veri merkezlerinin sahip olması gereken kriterler:

- Saklayıcı kuruluşun en az iki farklı şehirde ve beyaz alan üzerinde veri merkezi hizmeti yönetimi tecrübesi bulunmalıdır.
- Özel entegratör veya mükelleflerin sisteme yükleyeceği e-defterler, saklayıcı kuruluşun, iki veri merkezi üzerinde yedeklenerek bulundurulmalıdır.
- Veri Merkezi binası Saklayıcı Kuruluşa ait olmalıdır veya Başkanlığa başvuru tarihinden itibaren en az 10 yıl kullanım hakkına sahip olmalıdır.
- Veri Merkezlerinin her ikisinin de Deprem Yönetmeliği'ne uygun sağlamlaştırma çalışmalarının yapılmış olması, Saklayıcı Kuruluşunun yapılan çalışmaları belgelendirmesi ve her iki veri merkezi için Deprem Yönetmeliği'ne uygunluk belgesinin Başkanlığa sunulması gerekmektedir.
- Başkanlık, saklayıcı kuruluş veri merkezlerinde tutulan verilere 7/24 erişim halinde olacaktır. Bu nedenle GİB veri merkezi ile saklayıcı kuruluşun veri merkezleri arasında başlangıç olarak en az 100 Mbps hızında bağlantı sağlanmalıdır. Yine aynı altyapı, e-Defterlerin ikincil kopyalarının mükellefler tarafından saklayıcı kuruluşa gönderimi için kullanılacak bağlantılara da sorunsuz erişimi sağlayacak kapasitede olacaktır. Bu çerçevede kurulacak bağlantı zaman içerisinde Başkanlığın talep ettiği hız artırımlarına imkan tanır nitelikte olacaktır.
- Saklayıcı Kuruluş M/E erişim hizmetinin cihaz konfigürasyonları ve işletmesini yapacaktır.
- Saklayıcı Kuruluşun, arıza bildirimi için bir çağrı merkezi olacaktır. Çağrı merkezi, 7/24 esasına göre çalışacak ve bildirilen sorunları tarih ve saati ile beraber kayıt altına alabilecek donanıma sahip olacaktır.
- Saklayıcı kuruluşun Veri merkezilerinin enerji altyapısı ve yönetimi en az TIER 3 standartlarını sağlar nitelikte olmalıdır.
- Veri merkezlerinin topraklama ölçümlerinin 6 ayda bir yapılmalı ve EMO'nun (Elektrik Mühendisleri Odası) belirttiği değerlerde olmalıdır.

- Veri merkezlerinin iklimlendirme sistemleri asgari TİER 3 Standartlarına uygun olmalıdır.

- Saklayıcı kuruluşlar veri merkezlerinin fiziksel güvenliğini sağlamakla yükümlülerdir. Veri merkezlerinin bulunduğuna dair tabela, afiş gibi bilgilendirme sistemleri bulunmamalıdır. Kampüsü çevreleyen yeterince yüksek, üzerinde dikenli tel bulunan beton duvarlar bulunmalıdır. Kampüsü çevreleyen duvarlar üzerinde gece ve gündüz görüş kamera sistemi bulunmalıdır. Kameralar 7x24 kayıt yeteneğine sahip olmalı ve kamera kayıtları asgari 6 ay süre ile saklanmaktadır. Veri merkezi girişinde, kampüse giren kişiler ve araçlar için bir güvenlik bulunmalıdır. Veri merkezlerinin girişte bariyer sistemi bulunmalı, girişte 7x24 güvenlik sorgulaması yapılmalı, kampüse giren yabancı araçlar için bagaj kontrolü yapılmalıdır. Veri merkezi binasına girişte manyetik kartlı geçiş sistemi bulunmalı ve ziyaretçiler binaya X ray cihazından geçerek girebilmelidir. Beyaz alana tüm giriş ve çıkış kayıtları tutulmalıdır ve asgari 1 yıl süre ile saklanmalıdır Beyaz alan kameralar ile izlenmeli; kameralar kabinlerin bulunduğu koridorları, her iki uçtan kabin ve arkalarını görecek şekilde olmalıdır. Kamera görüntüleri en az 6 ay geriye yönelik saklanmalıdır. Gelir İdaresinin talebi sonrasında ilgili kayıtlar Gelir İdaresi'nin denetim amacıyla yerinde gösterilmesi veya Başkanlığa sunulması gerekmektedir.

- Veri Merkezi beyaz alanı içerisinde Gelir İdaresi tarafından talep edilmesi halinde kullanılacak bir kafes alanı sağlanacaktır. Kafes alanı veri merkezi yükseltilmiş tabanının üzerinde (yükseltilmiş taban altından insan geçişine imkan vermemeli) bir koruma sağlamalı ve tek bir soğuk hava koridoru içerisinde bulunmalıdır. Kafes alanı girişinde kullanılan kapılar için girişte parmak izi okuyucu veya kart okuyucu, çıkışında (iç tarafta) kart okuyucu bulunmalıdır. Kafes alanına giriş için yetkilendirmeler sadece saklayıcı kuruluş operasyon ekipleri için yapılmalıdır. Kafes alanı içerisi kamera ile izlenecektir ve İdare tarafından İdareye ait kabinetleri görecek açıda ayarlanacaktır.

- Veri merkezi ve kampüs çevresinde patlama ve yanma riski yüksek bir tesis bulunmamalıdır. Veri merkezi binası için yangın algılama ve söndürme sistemi bulunmalıdır. Veri merkezi beyaz alanı için sistemlere ve personele zarar vermeyecek yapıda uluslararası standartlara uygun yangın algılama ve söndürme sistemi bulunmalıdır. Acil çıkış kapısı/kapıları olmalıdır. Gerekli ışıklandırma ve yönlendirmeler içeride yapılmış olmalıdır.

- Sel baskınına karşılık sağlanacak veri merkezi beyaz alanı binanın bodrum katında bulunmamalıdır. Veri merkezi beyaz alanın bulunduğu binanın sel baskınına karşı koruması için kampüs çevresinde engel bulunmak zorundadır.

- Veri merkezi beyaz alanının bulunduğu binada herhangi bir noktadan su sızıntısı, damlama ve akıntı (çatı dahil) olmamalıdır.

- Veri merkezi beyaz alanın üzerinde ıslak zemin bulunmaması esastır. Bununla birlikte ıslak zemin bulunduğu hallerde, saklayıcı kuruluş bu hususta aldığı tedbirleri Başkanlığa göstermek zorundadır.

- Binada haşere ve farelere karşı önlem alınmalıdır ve düzenli olarak ilaçlanmalı ve 3 er aylık dönemlerde muayene kontrol listeleri Başkanlık ile paylaşılmalıdır.

- Veri merkezi için yıldırım tehlikesine karşı önlemler alınmış olmalıdır.

- Saklayıcı kuruluş, İdare ile 6 ayda bir olmak üzere veri merkezi içerisinde kullanılan ekipmanlar için periyodik kontrol ve bakımlarının formlarını paylaşmak zorundadır.

5.2 Veri Merkezi Beyaz Alan Özellikleri

- Veri merkezi soğuk hava kapalı koridora sahip olması gerekmektedir. Veri merkezi iklimlendirmesi ASHRAE 2008 standartlarında olması ve bölüm bazında iklimlendirme yedekliğinin nasıl sağlandığının Başkanlığa başvuru evrakında raporda detaylı olarak açıklanması gerekmektedir.

- Kullanılacak kafes alanı içerisinde İdare tarafından onaylanacak yapısal kablolama topolojisine göre kabin bazında 48 port bakır ve 24 port fiber yapısal kablolama saklayıcı kuruluş tarafından gerçekleştirilecektir.

- Yükseltilmiş döşeme yüksekliği standartlara haiz olmalıdır.

- Yükseltilmiş döşeme altı, epoksi ile kaplanmış olacaktır.

- Veri merkezi beyaz alan nem değeri /iklimlendirme standardı, ASHRAE 2008 standartlarına uygun olmalıdır.

5.3 Veri Merkezi Hizmetleri

Uzaktan destek ve destek hizmetleri:

- Veri merkezinde 7/24 tüm resmi ve dini bayramlar da dahil olmak üzere kesintisiz olarak hizmet verilecektir.
- Veri merkezinde bulunan operasyon ekibi, ihtiyaç durumunda yerel destek gereken noktalarda yerinde destek vermelidir.

İzleme Hizmetleri

- Ortam sıcaklık değeri izlenmeli, raporlanabilmeli, değer aşımları için alarm mekanizması bulunmalıdır.
- Ortam nem değeri izlenmeli, raporlanabilmeli, değer aşımları için alarm mekanizması bulunmalıdır.
- Jeneratörlere ait yakıt depoları seviyesi standart süreç ya da otomasyon ile izlenmelidir.
- Veri merkezi beyaz alan için minimum 2 saatte bir fiziksel ve görsel kontrol süreci bulunmalıdır.
- Veri merkezindeki operasyon ekibi 7x24 zaman diliminde asgari her 3 saatte bir genel kontrol gerçekleştirecektir.
- Veri merkezinde Enerji ve iklimlendirme ekibi 7x24 zaman diliminde asgari her 3 saatte bir genel kontrol gerçekleştirecektir.
- Veri merkezinde güvenlik ekibi 7x24 zaman diliminde asgari her 3 saatte bir genel kontrol gerçekleştirecektir.
- Veri merkezi içerisinde PDU'ya kadar tüm enerji tüketimlerini ve IT Ekipmanları ve Servisleri dâhil tüm sistemlerin ayakta çalışır halde bulunduğunu izleyecek BMS ve DCIM sistemleri bulunmalıdır.

5.4 Önleyici Bakım Hizmetleri

- Saklayıcı kuruluş, tüm ekipmanların (Trafo, Jeneratör, UPS, Klima-İç ve Dış Üniteler, Elektrik Panoları, Yangın Algılama ve Söndürme Sistemleri, Geçiş Kontrol Sistemleri, Kapalı Devre TV Sistemleri, …vb) bakım anlaşmalarını yaparak ve bakım sözleşme asıl ya da noter onaylı örneklerini idare ile paylaşmalıdır.

- Tüm enerji ve altyapı ekipmanları kontrolü için veri merkezinde 7/24 personel bulundurulmalı ve 3 saatte bir kontrol yapılmalıdır.

5.5 Veri Merkezi Ofis Alanı

- Veri merkezi ile aynı kampüs içerisinde 6 kişilik kapalı ofis alanı sağlanacaktır.
- Ofis alanı ile birlikte mobilya ve yerel alan ağı da sağlanacaktır
- Ofis alanına giriş bina girişinde kullanılan kartlar ile sağlanacaktır
- Ofis kapısında kullanılan kart okuyucu merkezi güvenlik sistemi ile entegre olup merkezi olarak yetkilendirme ve raporlamalar gerçekleştirilebilecektir.
- Ofis alanı içerisinde her bir masada 2xenerji ve 1xbakır network kablolama yapılmış olacaktır.

5.6 Erişim Altyapısı

Saklayıcı kuruluş tarafından İdarenin talebi doğrultusunda Veri Merkezi Internet, Veri Merkezi MPLS VPN, Noktadan Noktaya Bağlantı hizmetlerinden herhangi biri veya tümünü İdarenin kullanımına sunulacaktır.

5.7 İşletim ve Hizmet Süreçleri

- Saklayıcı Kuruluş 7x24 hizmet veren bir çağrı merkezine sahip olacaktır.
- Saklayıcı Kuruluş, arıza kaydı ve takibinin yapılabileceği çağrı merkezinin tüm iletişim bilgilerini Başvuru evrakında sunacaktır. İdare bu çağrı merkezine 7/24 esasına göre arıza bildiriminde bulunabilecektir. Arıza bildirimi telefon veya e-posta ile yapılabilecektir.
- Saklayıcı Kuruluş, proje aşamasında veya hizmetin sağlanması esnasında kritik öneme sahip bir sorun oluşması halinde iletişime geçilecek kişilerin kimlik bilgileri ve kendilerine erişilebilecek sabit ve cep telefonu bilgileri başvuru evrakında belirtilmelidir.
- İdarenin yapacağı felaket kurtarma veya acil müdahale kapsamına giren olağan üstü haller senaryolarında, Saklayıcı Kuruluş Başkanlığın vereceği tatbikat planına uyacaktır.

5.8 Servis Seviyeleri (SLA)

Saklama hizmeti kapsamında sunulacak veri merkezinin erişilebilirlik oranı en az %99,8 olmalıdır.

5.9 Saklayıcı Kuruluş Sertifikasyonlar

Saklayıcı Kuruluş Başkanlıkça kendisine verilen e-Defter saklama izni süresince aşağıdaki sertifikasyonlara ve niteliklere haiz olmalıdır.

- ISO 27001 Bilgi Güvenliği ve Yönetimi
- ISO 9001 Kalite Yönetim Sistemi

- ISO 20000 Bilgi Teknolojileri Hizmeti Yönetim Sistemi
- ISO 10002 Müşteri Memnuniyeti
- Veri Merkezlerinden en az bir tanesinde Uptime Institute TIER3 Design sertifikası bulunmalıdır.

Saklayıcı Kuruluş Başkanlıkça kendisine izin verilmesinden önce ilgili sertifikasyonlara sahip olduğunu idareye belgelendirmek zorundadır.

6. BELGELEME

e-Defter Saklama Hizmeti kapsamında uygulanan tüm yöntemler ve bu yöntemlerin tercih edilme gerekçeleri belgelenmeli, yöntem hiçbir gerekçe ile gizli tutulmamalıdır.

İşletici Kuruluş tarafından başvuru sırasında merkezi sistemine ilişkin aşağıdaki dokümanlar Başkanlık ile paylaşılmalıdır:

- Sistem Mimarisi
- Servis Mimarisi ve Teknik Akışlar
- Sunucu Mimarisi ve Donanım Altyapısı
- Depolama Kapasitesi
- Bağlantı Kapasitesi
- Sızma Test Raporu

Mükelleflere sunulacak tüm ekranların açık ve anlaşılır şekilde Kullanım Kılavuzu ile desteklenmesi kapsamında kullanım belgeleri sağlanmalıdır.

7. DEĞERLENDİRME VE İZİN

Başkanlık yapılan başvuruları 1 Sıra No.lu Elektronik Defter Genel Tebliği ile bu kılavuzda yapılan açıklamalara uygun olarak hazırlanacak Bilgi İşlem Sistem Raporunu değerlendirecek, gerek görmesi halinde teknik altyapının yeterliğini değerlendirmek amacıyla mükellefin bilgi işlem sistemini yerinde inceleyebileceği gibi yetkilendireceği kurum ya da kuruluşlarca incelenmesini isteyebilecektir.

Başkanlık iş bu kılavuzda belirtilen niteliklerin tamamına haiz olmayan saklayıcı kuruluş adaylarınca yapılacak başvurularda, eksik nitelikler ile ilgili olarak ayrıntılı plan ve taahhüt almak suretiyle başvuruyu kabul edebilir.

Yapılan değerlendirme neticesinde yeterli görülen mükelleflerle "Saklayıcı Kuruluş" çalışmalarına başlanacaktır. Kendilerine saklayıcı kuruluş izni verilenlerin listesi www.edefter.gov.tr internet adresinde yayımlanacaktır.

Mezkur Genel Tebliğ ve bu kılavuz kapsamında kendisine saklayıcı kuruluş izni verilen mükelleflerin, iş bu kılavuz çerçevesinde haiz olması gereken nitelikleri taşımadığı ya da zaman içinde yitirdiği tespit edilmesi halinde, kendisine verilen izin iptal edilebilecektir. Bu durumda saklama hizmeti verdiği mükelleflere ilişkin mevcut verilerin, ne şekilde ve hangi usul ile Başkanlığa ya da başka bir saklayıcı kuruluşa aktarılacağı ile ilgili olarak detaylı bir plan sunulmak zorundadır.

Kendisine "Saklayıcı Kuruluş" izni verilenler, herhangi bir nedenle söz konusu izinlerini kaybetmeleri durumunda, en az 2 yıl süre ile tekrar izin almak için İdare'ye başvuramazlar.