T.C. 
MİLLİ EĞİTİM BAKANLIĞI
Özel Öğretim Kurumları Genel Müdürlüğü

Sayı : 35235946/410.07/2296439
Konu: Kimlik Doğrulama Sistemi.

05/06/2014

................ VALİLİĞİNE
(İl Millî Eğitim Müdürlüğü)

İlgi : 18/05/2012 tarihli ve 28296 sayılı Resmi Gazete’de yaymlanarak yürürlüğe giren Millî Eğitim Bakanlığı Özel Eğitim Kurumları Yönetmeliği.

Bakanlığımıza bağlı özel eğitim ve rehabilitasyon merkezlerinde engelli bireylere verilen destek eğitimleri ile bu eğitimlerin giderlerinin Bakanlığımıza ödenmesine ilişkin iş ve işlemlerinin ilgi Yönetmelik hükümleri doğrultusunda yürütülüğü bilinmektedir.

İlgi Yönetmelinin 25 inci maddesinin 3., 4. ve 5 inci fıkralarda engelli bireylerin ve eğitim personelinin ders devam takiplerinin engelli birey modülünde yer alan kimlik doğrulama sistemi ile yapılacağı, engelli birey ile eğitim personelinin kimlik doğrulama sistemine tanıtımının rehberlik ve araştırma merkezlerinde yapılacağı, 30. inci maddesinde edemiş olasılık belgeler arasında kimlik doğrulama işlemi de yapan engelli birey modülündeki alınmış liste çıkıtıının olması gerektiğini hüküm altına alınmıştır. Ayrıca Yönetmelinin 34. üçüncü maddesinin birinci fıkrasının (a) bendi ile de 25. inci maddenin 3., 4. ve 5. inci fıkralarının yürürlüğe girmesi süresi 18.05.2012 tarihinden itibaren üç yıl olarak belirlenmiştir. Buna göre söz konusu hükümlerinkle genelinde en geç 18.05.2015 tarihinde yürürlüğe girecektr.

Yukarıda yer alan ilgi Yönetmelik hükümleri doğrultusunda faaliyet gösteren özel eğitim okullarının özel eğitim ve rehabilitasyon birimleri, özel eğitim ve rehabilitasyon merkezleri ve rehberlik araştırma merkezlerinde kurulması gereken engelli birey modülü ile uyumlu kimlik doğrulama sistemi için kurumların hazırlanaları gereken teknik alt yapısı (kablo, internet vb.) ile kurumlarda kullanılacak olan kimlik doğrulama cihazlarının hangi teknik özelliklerde olması gerektiğini (işlemci, işlemci işlem ünitesi (BlackBox vb.) ile ilgili bilgiler, ekte yer almaktaar. Ayrıca kimlik doğrulama sistemi ile engelli bireylerden alınacak olan saýsallaştırma kimlik verisinin güvenli bir şekilde Bakanlığımız sistem odasında bulunan sunuculara erişebilmesi için sanal özel ağ (VPN) erişiminin de sağlanması gerekmektedir. Bu kapsamda, özel eğitim ve rehabilitasyon merkezlerinin sanal özel ağ (VPN) hatti çekirdek doğrulama ünitesi bileşenlerini sisteme bağlamaları ve doğrulama sistemini kullanıma hazır hale getirmesi gerekmektedir. Söz konusu kimlik doğrulama sistemi ile ilgili uygulamaya ekte yer alan illerde başlanacaktır.

Bu belge, 5070 sayılı Elektronik İmza Kanununun 5 inci maddesi gereğince güvenli elektronik imza ile imzalanmıştır

MEB KAMPÜSÜ 06500 E-B BLOK BEŞEVLER ANKARA
Elektronik Ağ:oookgm@meb.gov.tr
e-posta: oookgm@meb.gov.tr

Ayrıntılı bilgi için Eğ.Uzm: Selahattin KOMAN
Tel: (0 312) 413 34 36
Faks: (0 312) 212 24 61
Diğer illerde Yönetmeliğin söz konusu hükümlerinin uygulama tarihleri ileride bildirilecektir. Ayrıca, 01 Temmuz 2014 tarihinden itibaren uygulamanın başladığı illerden 22 Temmuz 2014 tarihine kadar uygulamada karşılaşılan durumlara ilişkin raporun Bakanlığıma gönderilmesi gerekmektedir.

Bilgilerinizi ve gereğini rica ederim.

Yusuf TEKİN
Bakan .a
Müşteşar

EK: 1-Açıklamalar ve Sistem Teknik Özellikleri. ( 5 sayfa )
2-Uygulama yapılacak illerin listesi (Ek2)

DAĞITIM: B Planı

Bilgi:
- Özel Eğitim ve Rehberlik Hizmetleri Genel Müdürlüğü
- Bilgi İşlem Dairesi Başkanlığı
<table>
<thead>
<tr>
<th>SIRA NO</th>
<th>İL ADI</th>
<th>UYGULAMA BAŞLANACAK TARİH</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BİLEÇİK</td>
<td>01 Temmuz 2014</td>
</tr>
<tr>
<td>2</td>
<td>ÇANKIRI</td>
<td>01 Temmuz 2014</td>
</tr>
<tr>
<td>3</td>
<td>KARABÜK</td>
<td>01 Temmuz 2014</td>
</tr>
<tr>
<td>4</td>
<td>KIRIKKALE</td>
<td>01 Temmuz 2014</td>
</tr>
<tr>
<td>5</td>
<td>YALOVA</td>
<td>01 Temmuz 2014</td>
</tr>
<tr>
<td>6</td>
<td>ARDAHAN</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>7</td>
<td>ARTVİN</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>8</td>
<td>BAYBURT</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>9</td>
<td>BURDUR</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>10</td>
<td>ERZİNCAN</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>11</td>
<td>İĞDIR</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>12</td>
<td>ISPARTA</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>13</td>
<td>KARS</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>14</td>
<td>KIRKLARELİ</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>15</td>
<td>KİLİS</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>16</td>
<td>NEVŞEHİR</td>
<td>01 Ağustos 2014</td>
</tr>
<tr>
<td>17</td>
<td>TUNCELİ</td>
<td>01 Ağustos 2014</td>
</tr>
</tbody>
</table>
AVUÇ İÇİ DAMAR İZİ YÖNTEMIYLE KIMLIK DOĞRULAMA SİSTEMİ BİLEŞENLERİVE HAZIRLANACAK ALT YAPıYA İLİŞKİN AÇIKLAMALAR

Özel Eğitim ve Rehabilitasyon Merkezlerinde (REM) kurulacak avuç içi damar izi yöntemiyle kimlik doğrulama sistemi (Bundan sonra "damar izi kimlik doğrulama sistemi" olarak ifade edilecektir) aşağıdaki açıklamalar doğrultusunda özel eğitim ve rehabilitasyon merkezleri (REM) tarafından hazırlanacaktır.

1. Kurulum İçin Gerekli Altyapı

1.1. Damar izi kimlik doğrulama sistemi için sistemin konumlandırılması uygun bir yer belirlenmelidir.

1.2. Damar izkimlik doğrulama sistemi, doğrulama işlemini rahatlıkla yapabileceğini bir bölümde bulunmalıdır.

1.3. Damar izi kimlik doğrulama sisteminin bağlanacağı 24 saat şebeke elektriği mevcut bulunan priz veya direkt olarak enerji panosundan 3x2,5 TTR kablo ile çekilmiş enerji hatti sağlanmalıdır. Muhtemel enerji kesintilerine karşı, sistemin 7 gün 24 saat esasına göre sürekli çalışmasını sağlayacak tedbir alınmalıdır.

1.4. Damar izi kimlik doğrulama sistemi ile kurulacak olan VPN hatti arasına CAT 6 kablo ile sağlanması gereken network bağlantısı oluşturulmalıdır.

1.5. Damar izi kimlik doğrulama sisteminin kurulumu aşamasında eğitim alacak personel hazır bulunurulmalı ve kurulmadan sonra sistemin eğitimi alınmalıdır.

2. Damar İz Kimlik Doğrulama Sistemi

2.1. Damar İz Kimlik Doğrulama Sistemi İstemci Donanımı

2.1.1. Damar izi kimlik doğrulama sistemi cihazı ile birlikte çalışması için gerekli tüm çevre birimleri/donanımlar temin edilmelidir.

2.1.2. Altyapı ve kablolama ürünü REM’ler tarafından hazırlananmış olacaktır.

2.1.3. Cihazın kurulumundan sonra çalıştırılması için gerekli tüm bilgilerkurumunun yapan firma tarafından, ilgili REM sorumlularına bildirilmelidir.

2.1.4. Cihaz arızaları için donanım değişimi yapılarak çözüm sağlanmalıdır.

2.1.5. Cihaz yazılım güncellemelerinin merkezi, otomatik ve güvenli şekilde yapılabilmelidir.

2.1.6. Cihazların online, offline vb. durumlarının merkezi sistem ile takip edilebilmesi sağlanmalıdır. Bu bir arı yüz ile kontrol edilebilecektir.

2.1.7. Cihazda oluşacak sorunların cihazın kolay, anlaşılır ve görüntülenebilir hata kodları üretmesi sağlanmalıdır.

2.1.8. Cihaz sorunları için kurum bünyesinde uzaktan destek verilmesine olanak sağlanmalıdır.

2.1.9. Cihaz ilk kurulum/devre alınma hizmeti standart olarak verilmelidir.

2.1.10. Cihazın fiziksel sorunlarından dolayı değişimi en fazla 2 günde sağlanmalıdır.

2.1.11. Cihaz en az 3 yıl standart garanti ile alınmalı, üretici firma/yüklenici tarafından 5 yıl yedek parça olarak sağlanmalıdır.
2.1.12. Cihazın yazılımı ile ilgili olarak 3 yıl süresi boyunca ücretsiz olarak bakım desteği verilmelidir.

2.2. Damar İzi Kimlik Doğrulama Sistemi-İstemci İşlem Ünitesi

2.2.1. Damar izi kimlik doğrulama sistemi (DİKDS)-İstemci işlem ünitesi; endüstriyel tipte olmalı, 7 gün 24 saat esasına göre ve 0°C ila 60°C sıcaklık aralığında kesintisiz olarak çalışabilirmelidir.

2.2.2. DİKDS-İstemci işlem ünitesi üzerinde fan bulunmayacaktır.

2.2.3. DİKDS-İstemci işlem ünitesi en az 1.20 GHz hızında, yüksek performanslı işlemciye sahip olacaktır.

2.2.4. DİKDS-İstemci işlem ünitesinde en az DDR31066 Mhz hızında 2 GB kapasiteli bellek olacaktır.

2.2.5. DİKDS-İstemci işlem ünitesinin en az 2 adet DIMM yuvası olacaktır.

2.2.6. DİKDS-İstemci işlem ünitesinin diski en az 2 GB kapasitede olacaktır. İstemci işlem ünitesine ait sabit disk ölçülüp başka bir sisteme takıldığında içerisindeki bilgilereerişim engellenmiş olacaktır.

2.2.7. DİKDS-İşleme işlem ünitesi; harici olarak farklı cihazlar ile boot edilemeyecektir.

2.2.8. DİKDS-İstemci işlem ünitesine harici olarak başka bir depolama aygıtı bağlanmasızdurumunda, bu aygıta sistem üzerinden herhangi bir depolamamıktan olmayacaktır.

2.2.9. DİKDS-İşleme işlem ünitesinde entegre şeklinde idarece istenecek bilgiler SAM modüllü bulunacaktır.

2.2.10. DİKDS-İşleme işlem ünitesi, kişinin TC kimlik no ve damar izi bilgilerini kriptolayarak ana sunucuya transfer edecek teknolojiye sahip olacaktır.

2.2.11. DİKDS-İstemci işlem ünitesinin, damar izi kimlik doğrulama okuma ünitesi ve istemci giriş çıkış ünitesiyle bağlantıdan endüstriyel tipte konnektörler kullanılarak bu sistem üzerinde 3 adet endüstriyel tipte bağlantılı noktası bulunacaktır. İstemci işleme ünitesinde bir adet RS232 portu bulunacaktır. RS232 portu endüstriyel tip konnektör olarak değerlendirilemeyecektir.

2.2.12. DİKDS-İstemci işlem ünitesi sadece damar izi kimlik doğrulama okuma ünitesi bağlantısını ve aynı anda sadece tek bir sayısallaştırılmış kimlik bilgisi teknolojisinin kullanılmasına izin verecektir.


2.2.14. DİKDS-İstемci işlem ünitesinde 10/100/1000 Mbit hız desteği ve PXE & Wake on LAN desteği sahip bir adet Ağethernet adaptörü olacaktır.

2.2.15. DİKDS-İstемci işlem ünitesi üzerinde uyari sinyali alınabilecek tipte buzzer bulunacaktır. İstenildiği zaman ses kapatabilecektir.

2.2.16. DİKDS-İstемci işlem ünitesi beslemesi için sistem kartı üzerinde bütünleşik halde DC-in portu olacaktır ve sistem, 19V-24V DC gerilim aralığında çalışacaktır.

2.2.17. DİKDS-İstемci işlem ünitesi; şebeke stmt voltaj dalgalanmalara karşı, ürünün stabilitesini sağlamanak adına voltaj sistemine sahip olacaktır.
2.2.18. DİKDS-İstемci işlem ünitesi; yetkisiz kişilerce, fiziksel olarak açılmaya karşı korunmalı olacaktır. Sistem, yetkisiz kişilerce açılsa dahi kendini bloke edecek ve çalışmasını durduracak şekilde tasarlanmış olacaktır.

2.2.19. DİKDS-İstемci işlem ünitesi; Elektromanyetik Uyumluluk Yönetmeliği (2004/108/EC) ile uyumlu olup aşağıdaki standartlara uygun olacaktır.

- EN 61000-3-3:2008

2.2.20 DİKDS – İstемci işlem ünitesi,Eko Dizayn Yönetmeliği (2009/125/EC) ile uyumlu olup aşağıdaki standartlara uygun olacaktır.

- EC No 1275/2008
- EN 62301:2005

2.2.21. DİKDS – İstемci işlem ünitesi; CE sertifikasına sahip olacaktır.

2.2.22. DİKDS – İstемci işlem ünitesi; RoHs uyuımlılığı olacaktır.

2.2.23. İstемci işlem ünitesi; WEEE uyuımlılığı olacaktır.

2.2.24. İstемci işlem ünitesi; Energy Star uyuımlılığı olacaktır.

2.2.25. DİKDS – İstемci işlem ünitesi; Avrupa Birliği Veri Koruma Direktifine (95/46/EC)uyumlu olacaktır.

2.2.26. DİKDS – İstемci işlem ünitesi ile ilgili tüm sertifikalar ürünlerle birlikte kuruma teslim edilmelidir.

2.3. Damar İzi Kimlik Doğrulama Sistemi – İstемci Giriş-Çııkış Ünitesi

2.3.1. DİKDS – İstемci giriş-çııkış ünitesinde en az 3 inch ve 640x480 ekran çözünürlüğündedekleyen renkli TFT ekran bulunacaktır.

2.3.2. DİKDS – İstемci giriş-çııkış ünitesinde kullanıcının TC kimlik bilgisini girmesine olanaktanyacak 0, 1, 2, 3, 4, 5, 6, 7, 8, 9*, Sil, İplad, Giriş tuşları, 4 adet navigasyon tuşu ve F1, F2,F3, F4 programlanabilir fonksiyon tuşlarını içeren klavye bulunacaktır.

2.4. Damar İzi Kimlik Doğrulama Sistemi – Okuma Ünitesi

2.4.1. DİKDS – Okuma Ünitesi; damar haritasını okuma ve kendi üzerinde AES 256 bitalgoritma ve anahtar uzunluğu ile şifreleme özelliklerine sahip olmalıdır.

2.4.2. DİKDS- Okuma Ünitesinden veri çıkışı (Elektronik devreveye USB arabirimine) tamamen güvenli ve şifreli olmalıdır. Bu verinin tüm arabirimler arası iletişimde veri şifreli olarak taşınmalıdır. Verinin üretmesi ile veri merkezinde doğrulamasına kadar her aşama (uçtan uca) güvenli olmalıdır.

2.4.3. DİKDS- Okuma Ünitesi tekel ve değiştirilemez bir tamamlayıcıya sahip olmalıdır. Bu sayede merkezi olarak onay verilmemiş sistemlerin kullanımı engellenebilmeli ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilimelidir.

2.4.4. DİKDS- Okuma Ünitesi mümkün olduğuguna düzenli temizlik gerektirmemeli, toz, kir, yağ gibi çevresel faktörlerden etkilenmemeli. İşık altında çalışabilimelidir.

2.4.5. DİKDS- Okuma Ünitesi; İnsan sağlığına zararlı ırrın sınıftında olmamalıdır.

2.4.6. DİKDS- Okuma Ünitesi’nin FAR (Felsefe Acceptance Rate) değeri % 0,00008 ve FRR (False Rejection Rate) değeri % 0,01’den büyük olmamalıdır.

3
2.4.7. DİKDS bahsedilen FAR ve FRR değerlerini tek bir sayısallaştırılmış kimlik bilgisi okuyucu ve tek bir sayısallaştırılmış kimlik bilgisi yöntemi ile sağlamalıdır. Bu değerler birden fazla sayısallaştırılmış kimlik bilgisi teknolojisinin birleşimi ile sağlanmayaaktır.

2.4.8. DİKDS- Okuma Ünitesi, merkezi olarak (online) 1:1 ve 1:N kimlik doğrulamaya, sistem ilave herhangi bir tasma depolama materyali olmaksızın imkan sağlamalıdır.

2.4.9. DİKDS- Okuma Ünitesi, canlı doku tespit (Life Detection) özelliğine sahip olmalıdır.

2.4.10. DİKDS- Okuma Ünitesi; enerjisini USB 2.0 üzerinden almalı ve maksimum 2.5 Wattenerji tüketimi olmalıdır.

2.4.11. DİKDS- Okuma Ünitesi’nin çalışma sıcaklık aralığı 0-60 °C olmalıdır.

2.4.12. DİKDS- Okuma Ünitesi tamamı olduğu istemci ünitesinden çıkarılıp başka bir istemci ünitesine takıldığında çalışmamalıdır.

2.5. Damar İzi Kimlik Doğrulama Sistemi – Konumlandırma Ünitesi

2.5.1. DİKDS- Konumlandırma Ünitesi; Damar İzi Kimlik Doğrulama – Okuma Ünitesi ile entegreolmalıdır.

2.5.2. DİKDS- Konumlandırma Ünitesi; 6 yaş üstü ve eğitim grubundaki bireylerin rahatlıkla kullanımların imkan verecek, kullanılabilecek olan uzun ergonomik yapısı uygun, Damar İzi Kimlik Doğrulama – Okumasını kolaylaştırır, hatası en aza indiren ve Damar İzi Okuma Ünitesi teknik gereksinimlerine uygun tasarदında olmalıdır.

2.6. Damar İzi Kimlik Doğrulama Sistemi – İstемci Yazılımı – İşlem Ünitesi

2.6.1. DİKDS-İstемciyazılımı, Sistemin merkeze erişebilmesi için gerekli IP, SubnetMask, Gateway, DNS Server gibi bilgilerin girilmesine imkan sağlamalıdır.

2.6.2. DİKDS-İstемciyazılıımı, İstемci ID’lerinin ve şifrelerinin girilmesine imkan sağlamalıdır.

2.6.3. DİKDS-İstемciyazılıımı, sistemin network ve merkeze erişebilirliğini tespit edilmesi için kullanımmı kolay network tanımlama araçlarına sahip olmalıdır.

2.6.4. DİKDS-İstемciyazılıımı, merkez sistem üzerinden istenildiği zaman güncellenebilmelidir.

2.6.5. DİKDS-İstемciyazılıımı, KeyPad‘den girilen komutlara göre sayısallaştırılmış kimlik doğrulama ve sayısallaştırılmış kimlik bilgisi kayıt işlemlerini gerçekleştirecek, işlem adımlarını, operatörden üzerindeki ekranın takip etmesini sağlayacak, sayısallaştırılmış kimlik bilgisinin görüntüstünün alınması sırasında görüntülenme yapacak şekilde tasarlanmalıdır.

2.6.6. DİKDS-İstемciyazılıımı, sunucu yazılımı ile SecureSocketLayer üzerinden ve en az 128bit anahtar uzunluğu kullanılarak iletişime geçektir.

2.6.7. DİKDS-İstемciyazılıımı, güvenlik sebebi ile sayısallaştırılmış kimlik bilgileri, sensörün içerisinde AES, Blowfish, DES, TripleDES, Serpent, Twofish gibi dünyada kabul görmüş simetrik şifreleme algoritmaları ile ve en az 256 bit şifre anahtar uzunluğu kullanılarak şifrelemlidir.

2.6.8. DİKDS-İstемciyazılıımı, güvenlik sebebi ile okuyucu sensör ile istemci cihazı arasındaki sayısallaştırılmış kimlik bilgisi içerisinde AES, Blowfish, DES, Triple DES, Serpent, Twofish gibi dünyada kabul görmüş simetrik şifreleme algoritmaları ile ve en az 256 bit şifre anahtar uzunluğu kullanılarak şifreleme yapacak şekilde iletişim belirlidir.

2.6.9. Okuyucu sensör, okuma işlemlerinin hemen ardından, sayısallaştırılmış kimlik bilgisi istemci cihaza gönderilmeden sayısallaştırılmış kimlik bilgilerini geri dönüştümsüz bir algoritmadan geçirerek, orijinal sayısallaştırılmış kimlik bilgisi görüntüstünün tutmayıacak ve daha
sonra istemci cihazına sayısallaştırılmış kimlik bilgisini iletecektir, algoritmadan geçirilen veriden orijinal sayısallaştırılmış kimlik bilgisi imajına dönülmesi mümkün olmayacaktır.

2.6.10. DIKDS-Istemciyazılımı, ilk kayıt ve ilk doğrulama esnasında alınan ve doğrulanan kaydın kalitesini değerlendirebilecek, alınan sayısallaştırılmış kimlik bilgisi kalitesi yeterli değil ise, sayısallaştırılmış kimlik bilgisi kaydın merkeze gönderilmeden önce yenilenebilmesine imkan sağlayacaktır.

2.6.12. DIKDS-Istemciyazılımı, belirlenecek özel durumların merkeze bildirilmesine imkan sağlayacak altyapıda olacaktır. (Örneğin,bireyin bir elinin olmaması gibi)

2.6.12. DIKDS-Istemciyazılımı, bir ait TC kimlik numaralarının hatalı girilmesini engelleyecek yazılımsal kontrollere sahip olmuştur.

2.6.13. DIKDS-Istemciyazılımı, kurum işlemi sırasında kurum bilgilerinin değiştirilmesi durumunda merkez ile iletişime geçip, aktivasyon işlemi yapılmadan kayıt doğrulama işlemi yapılmasına imkan vermeyecektir.


2.6.15. DIKDS-Istemci sistemi veyazılımını üzerinde kesinlikle kalıcı olarak sayısallaştırılmış kimlik bilgisi bulundurulmayacak ve işlenemeyecektir. İlk kayıt veya doğrulama amaçtı sayısallaştırılmış kimlik bilgisi alınır alınmaz güvenli bir şekilde merkezi sunucu yazılımlına iletecektir. Sayısalıştırılmış kimlik bilgisinin doğru olup olmadığını karar verme işlemi merkezi sunucu yazılımı üzerinde güvenli ortamda yapılacak, istemci yazılımına sadece onay bilgisi gönderilecektir.

2.6.16. DIKDS-Istemciyazılımı ve istemcinin çalışması için herhangi bir başka bilgisayar ve yazılıma gerek duyulmayaçak, sistem kendi başına stand-alone çalışanacak yapıda olmuştur.

2.6.17. DIKDS-Istemci işlem ünitesi veri çıkış (Ethernet kartı ) tamamen güvenli ve şifreli olacaktır. Bu verinin tüm arabirimler arası iletiminde veri şifreli olarak taşınmalıdır. Verinin türtilmesi ile veri merkezinde doğrulanmasına kadar her aşama (uçtan uca) güvenli olmalıdır. HTTPS ile şifrelenir ve veri merkezde bulunan SSL Offloading VPN cihazında açılacaktır.

2.6.18. DIKDS-Istemci işlem ünitesinde Ethernet kartına çıkarılan veri merkeze MPLS VPN ile kurum arasında çözüleme imzalandıktan sonra planlanacaktır.