BİYOMETRİK YÖNTEMLERLE KİMLİK DOĞRULAMA SİSTEMLERİNE AİT KILAVUZ

Bilindiği üzere 5510 sayılı Kanunun 67'nci maddesinin üçüncü fıkrasında yer alan hükme göre sağlık hizmeti almak için sağlık hizmeti sunucularına başvuran kişilerin kimlik doğrulamaları, nüfus cüzdanı, sürücü belgesi, pasaport veya evlilik cüzdanı ile yapılmaktaydı.

Ancak hizmet sunumunda vatandaşların kimliğinin geleneksel yöntemler ile doğru olarak saptanamamasının getirdiği sorunların önlenmesi amacıyla; kişilerin TC kimlik numarası bulunan nüfus cüzdanı, sürücü belgesi, pasaport veya evlilik cüzdanı ve/veya biyometrik yöntemlerle kimlik tespit işlemleri tamamlandıktan sonra sağlık hizmeti sunucusundan sağlık hizmeti almalarına ilişkin 1/3/2012 tarihli ve 6283 sayılı Kanunun 1 inci maddesiyle 5510 sayılı Kanunun 67 nci maddesinin 3 üncü fıkrasında düzenleme yapılmıştır.

Ayrıca Sağlık Uygulama Tebliğinin 3.1.2 numaralı maddesinde yapılan değişiklikle; sağlık kurum ve kuruluşlarının, Kurum sağlık yardımlarından yararlandırılan kişilerin kendilerine müracaatı aşamasında (acil hallerde ise acil halin sona ermesinden sonra) nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya verilmiş ise Kurum sağlık kartı belgelerinden biri ile kimlik tespiti ve biyometrik yöntemlerle kimlik doğrulaması yapmaları zorunlu hale getirilmiş olup ayrıca kimlik tespiti, biyometrik kayıt işlemi veya biyometrik kimlik doğrulama işlemini usulüne uygun yapmayan ve bu nedenle bir başka kişiye sağlık hizmeti sunulması nedeniyle Kurumun zarara uğramasına sebebiyet veren sağlık hizmeti sunucularından ödenen tutarın geri alınacağı hüküm altına alınmıştır.

Yine Sağlık Uygulama Tebliğinin, "Biyometrik kimlik doğrulama işlemi" başlıklı 3.1.2.A. maddesinde; Kimlik doğrulamada kullanılacak olan biyometrik sistem ve uygulamaya geçilecek sağlık hizmeti sunucuları, uygulama tarihi ile uygulamaya ilişkin usul ve esasların Kurum tarafından belirleneceği, Kurum sağlık yardımlarından yararlandırılan kişinin sağlık hizmeti sunucusuna müracaatı sırasında ilk biyometrik verinin Kurum veri tabanına kayıt işleminin sağlık hizmeti sunucusu tarafından yapılacağı da belirtilmektedir.

Belirtilen bu hususlar çerçevesinde; Kurumumuz tarafından pilot uygulaması yapılan ve başarı ile sonuçlanan Biyometrik Kimlik Doğrulama Yöntemlerine ait düzenlemeler aşağıda yer almaktadır.

1. Tanımlar

1.1. Genel sağlık sigortalısı: 5510 sayılı Kanunun 60 ıncı maddesinde sayılan kişiler ile bu kişilerin yine aynı Kanunun 3 üncü maddesinin 10 uncu fıkrasında belirtilen bakmakla yükümlü olduğu kişileri,

1.2. Kurum: Sosyal Güvenlik Kurumu Başkanlığını,

1.3. Sağlık Hizmeti: Genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilere Kanunun 63 üncü maddesi gereği finansmanı sağlanacak tıbbî ürün ve hizmetleri,

1.4. Sağlık Hizmeti Sunucusu: Sağlık hizmetini sunan ve/veya üreten; üniversitelere bağlı hastaneler ile 2. Basamak özel sağlık tesisleri,

1.5. İlk kayıt: Genel sağlık sigortalısının, sağ ve sol eline ait avuç içi damar izi veya sağ ve sol eline ait sırasına göre, işaret, orta, yüzük, baş, küçük parmaklardan iki tanesine ait parmak damar izi, biyometrik verisinin kendisine ait TC kimlik numarasıyla eşleştirilmesi işlemi sonrasında oluşturulan kayıt işlemini,

1.6. Kimlik Doğrulama İşlemi: Genel sağlık sigortalısının, ilk kayıt işlemi sonrasındaki biyometrik verisi ile sağlık hizmet sunucusuna başvuru aşamasında alınması gereken sağ veya sol eline ait avuç içi damar izi veya sağ veya sol eline ait ilk kayıt sırasında kaydı alınan parmaklardan herhangi birisine ait parmak damar izi, biyometrik verisinin karşılaştırılması sonrasında kimlik tespitinin doğrulanmasını ifade eden ve sistem tarafından üretilen onaylama kodunu,

1.7. Biyometrik Sistemi: Ek:1'de teknik özellikleri ayrı ayrı belirtilen biyometrik kimlik doğrulama ünitelerinin bileşenlerini, ifade eder.

2. Biyometrik Sistemin uygulamasına ilişkin düzenlemeler

2.1. İlk kayıt ile ilgili işlemler

Genel sağlık sigortalısı, TC kimlik numarası bulunan nüfus cüzdanı, sürücü belgesi, pasaport veya evlilik cüzdanıyla sağlık hizmeti almak amacıyla sağlık hizmeti sunucusuna başvurularında biyometrik sistem ile ilk kayıt işlemi sağlık hizmeti sunucusu tarafından yapılacaktır. İlk kayıt işlemi yapılmadan önce biyometrik verisi alınacak kişinin yine sağlık hizmet sunucusu tarafından EK:2 de yer alan rıza formunun da imzalatılarak alınması gerekmektedir.

2.2. Kimlik doğrulama ile ilgili işlemler

İlk kayıt işlemi tamamlanan genel sağlık sigortalısının sağlık hizmeti sunucusuna müracaatında MEDULA takip numarası alınması işlemi öncesinde sağlık hizmeti sunucusu tarafından avuç içi damar izi veya parmak damar izi sistemi ile biyometrik kimlik doğrulaması yapılacaktır.

Bu kılavuzun 2.4 üncü maddesinde belirtilen istisnalar hariç olmak üzere sağlık hizmeti sunucusu tarafından belirtilen biyometrik kimlik doğrulama işlemi yapılmadan genel sağlık sigortalısı adına MEDULA takip numarası alınmasına MEDULA sistemi tarafından izin verilmeyecektir.

Sağlık hizmeti sunucusu tarafından genel sağlık sigortalısının, biyometrik kimlik doğrulaması yapıldıktan sonra genel sağlık sigortalısı adına MEDULA takip numarası alınarak sağlık hizmeti sunulmaya başlanacaktır.

2.3. Genel sağlık sigortalısının biyometrik verilerinin silinmesi

Genel sağlık sigortalısının, bu kılavuzun 2.1 inci maddesinde belirtilen ilk kayıt işleminin yanlış yapıldığının tespit edilmesi halinde genel sağlık sigortalısına ait biyometrik verileri Kurum tarafından silinecektir.

Biyometrik verisi silinen genel sağlık sigortalısı, bu kılavuzun 2.1 maddesinde belirtilen ilk kayıt işlemlerini, sağlık hizmeti almak amacıyla başvurduğu sağlık hizmet sunucusunda yaptırmak zorundadır.

2.4. Biyometrik kimlik doğrulaması yapılmayacak olan genel sağlık sigortalıları

2.4.1 12 yaş ve altı çocuklara, ~~65~~ **75** yaş ve üstü kişilere, **(13.08.2014 tarihli duyuru ile yapılan düzenleme, Yürürlük: 28.08.2014)**

2.4.2 Her iki üst ekstremitesi olmayan kişilere (elleri olmayan),

2.4.3 Her iki el avuç içi veya her iki el orta, işaret, yüzük, baş, küçük parmak damar izi bütünlüğü bozulmuş olanlara,

2.4.4 Acil hastalara (yeşil alan muayenesi hariç),

2.4.5 Serepral palsi, üst ekstremite felci ve benzeri tıbbi nedenlerden dolayı biyometrik verisi alınamayan kişilere, **spastik veya otistik engelli olan kişilere, (13.08.2014 tarihli duyuru ile yapılan düzenleme, Yürürlük: 28.08.2014)**

2.4.6 Organ, doku ve kök hücre nakli tedavilerinde alıcının üzerinden donör takibinin alındığı durumlarda,
bu kılavuzun 2.1 ve 2.2 inci maddelerinde belirtilen işlemler yapılmayacaktır.
Yukarıda belirtilen genel sağlık sigortalıları, nüfus cüzdanı, sürücü belgesi, pasaport ya da evlilik cüzdanlarıyla sağlık hizmeti sunucularına müracaat etmeleri halinde sağlık hizmeti alabileceklerdir.

2.5. Biyometrik kimlik doğrulaması yapılması gereken durumlar

Sağlık hizmeti sunucuları tarafından genel sağlık sigortalısı adına alınan her provizyonda, bu kılavuzun 2.2 nci maddesinde belirtilen kimlik doğrulamasının yapılması gerekmektedir. Genel sağlık sigortalısının ilk ayaktan başvuru sonrası, muayene, kontrol muayenesi ile **ayaktan veya günübirlik kapsamında yapılan** ESWL, ESWT, diyaliz (ev hemodiyalizi hariç), fizik tedavi, hiperbarik oksijen tedavisi işlemlerinin her seansında **ve günübirlik kapsamında alınan tüp bebek tedavisi takiplerinde** bu kılavuzun 2.2 nci maddesinde belirtilen kimlik doğrulaması yapmaları zorunludur. **(13.08.2014 tarihli duyuru ile yapılan düzenleme, Yürürlük: 28.08.2014)**

3. Sağlık hizmet sunucusunun sorumlulukları

3.1. Sağlık hizmeti sunucusu, genel sağlık sigortalısının kimlik doğrulama işlemlerini bu kılavuzun 2.1 ve 2.2 nci numaralı maddelerinde belirtilen hükümlere göre yapmaları zorunludur.

3.2. Bu kılavuzun 2.1 ve 2.2 nci maddelerine göre yapılması gereken işlemlerin yapılmaması ya da yanlış yapılması nedeniyle Kurumun usulsüz ve yersiz ödeme yapmasına sebebiyet verdiği tespit edilen sağlık hizmeti sunucusu hakkında mevzuat hükümlerine göre Kurum tarafından gerekli işlemler yapılacaktır.

4. Genel sağlık sigortalısının sorumlulukları

4.1. Genel sağlık sigortalısı, sağlık hizmeti sunucularına başvurusunda bu kılavuzun 2.1 ve 2.2 nci maddelerinde belirtilen işlemleri yaptırarak kimlik tespiti ve doğrulamalarını yaptırmak zorundadır.

4.2. Bu kılavuzun 2.1 ve 2.2 nci maddesinde belirtilen işlemleri yaptırmayan ve bu nedenle Kurumun yersiz ve usulsüz ödeme yapmasına sebebiyet veren genel sağlık sigortalısı hakkında mevzuat hükümlerine göre Kurum tarafından gerekli işlemler yapılacaktır.

5. Sistemin ülkeye yaygınlaştırılması

2.Basamak Özel Sağlık Hizmet Sunucuları 1.12.2013, üniversite hastaneleri ise 01.09.2014 tarihine kadar EK-1 de yer alan Biyometrik Sistemlerden birini seçerek Biyometrik Kimlik Doğrulama Sistemine geçişlerini tamamlayacaklardır.

6. Yürürlük

Bu kılavuz yayımlandığı tarihte yürürlüğe girer.
Kurumun internet sayfasında 14.09.2012 tarihinde yayımlanan kılavuz, 22.11.2012 tarihinde yayımlanan kılavuz değişikliği, 30.04.2013 tarihinde yayımlanan kılavuz ve 03.01.2013 tarihinde Sağlık Hizmet Sunucularına yapılan duyuru yürürlükten kaldırılmıştır.
Bilgi edinilmesini ve gereğini rica ederim.

EKLER:

EK 1. Biyometrik kimlik doğrulama ünitelerinin teknik özellikleri
1. TİP BİYOMETRİK KİMLİK DOĞRULAMA SİSTEMİ SEÇENEĞİ

Avuç İçi Damar İzi Sistemi Biyometrik Kimlik Doğrulama Ünitesinin Bileşenleri
2. TİP BİYOMETRİK KİMLİK DOĞRULAMA SİSTEMİ SEÇENEĞİ

Parmak Damar İzi Sistemi Biyometrik Kimlik Doğrulama Ünitelerinin Bileşenleri
Tip 2-A Parmak damar izi sistemi
Tip 2-B Parmak damar izi sistemi
Tip 2-C Parmak damar izi sistemi
Tip 2-D Parmak damar izi sistemi
EK 2. Rıza Formu

Op.Dr.Tonguç SUGÜNEŞ
Genel Müdür V

EK 1-(1)

1.TİP BİYOMETRİK KİMLİK DOĞRULAMA SİSTEMİ SEÇENEĞİ

Avuç İçi Damar İzi Sistemi Biyometrik Kimlik Doğrulama Ünitesinin Bileşenleri

1. İstemci donanımı

1.1. Cihaz ile birlikte çalışması için gerekli tüm çevre-birimler/donanım teslim edilecektir.

1.2. Altyapı ve kablolama ürünü satın alan sağlık hizmet sunucuları tarafından hazırlanmış olacaktır.

1.3. Cihaz devreye alınması sırasında gerekli olacak tüm bilgiler sağlık hizmet sunucuları tarafından belirlenmiş olan kurulum sorumlusuna iletilecektir.

1.4. Cihaz arızaları için donanım değişimi yapılarak çözüm sağlanacaktır.

1.5. Cihaz yazılım güncellemeleri merkezi, otomatik ve güvenli şekilde yapılabilmesi sağlanmalıdır.

1.6. Cihazların merkezi sistem ile takip edilebilmesi sağlanmalıdır.

1.7. Cihazda oluşacak sorunlar için kolay, anlaşılır ve görüntülenebilir hata kodları üretmesi sağlanmalıdır.

1.8. Cihaz sorunları için uzaktan destek verilmesine olanak sağlanmalıdır.

1.9. Cihaz ilk kurulum/devreye alınma hizmeti standart olarak verilmelidir.

1.10. Cihazın fiziksel sorunlarından dolayı değişimi en fazla 5 iş gününde sağlanmalıdır.

1.11. Cihaz 2 yıl standart garanti ile satışı yapılacak olup, 10 yıl yedek parça sağlanmalıdır.

1.12. Cihazlar, sevk esnasında sigortalı olarak taşınmalıdır.

2. İstemci işlem ünitesi (BlackBox)

2.1. İstemci işlem ünitesi; hastane - poliklinik - eczane gibi medikal alanlarda kullanılmaya elverişli özellik ve tasarıma sahip olacaktır.

2.2. İstemci işlem ünitesi; endüstriyel tipte olup, 7 gün 24 saat esasına göre ve 0°C ila 60°C sıcaklık aralığında kesintisiz olarak çalışabilecektir.

2.3. İstemci işlem ünitesi üzerinde fan bulunmayacaktır.

2.4. İstemci işlem ünitesi en az 1.20 GHz hızında, yüksek performanslı işlemciye sahip olacaktır.

2.5. İstemci işlem ünitesinde en az DDR3 1066 Mhz hızında 2 GB kapasiteli bellek olacaktır.

2.6. İstemci işlem ünitesinin en az 2 adet DIMM yuvası olacak, bellek yuvalarına aynı anda 2 adet 4 GB, en az 1066 Mhz hızında RAM takılarak sistemin en az 8 GB desteklediği görülecek, belleklerin tamamı 1066 Mhz çalışacaktır.

2.7. İstemci işlem ünitesinin diski en az 2 GB kapasitede olacaktır. İstemci işlem ünitesine ait sabit disk sökülüp başka bir sisteme takıldığında içerisindeki bilgilere erişim engellenmiş olacaktır.

2.8. İstemci işlem ünitesi; harici olarak farklı cihazlar ile boot edilemeyecektir.

2.9. İstemci işlem ünitesine harici olarak başka bir depolama aygıtı bağlanması durumunda, bu aygıta sistem üzerinden herhangi bilgi depolanması mümkün olmayacaktır

2.10. İstemci işlem ünitesinde entegre şekilde SAM modulü bulunacaktır.

2.11. İstemci işlem ünitesi, kişinin TC Kimlik No ve biyometrik kimlik bilgilerini kriptolayarak ana sunucuya transfer edecek teknolojiye sahip olacaktır.

2.12. İstemci işlem ünitesinin, Damar İzi Okuma Ünitesi ve İstemci Giriş-Çıkış Ünitesi ile bağlantısında endüstriyel tipte konnektörler kullanılacak ve sistem üzerinde en az 3 adet endüstriyel tipte bağlantı noktası bulunacaktır.

2.13. Black Box sadece Damar İzi Okuma Ünitesi bağlantısına ve aynı anda sadece tek bir biyometrik teknolojinin kullanımına izin verecektir

2.14. İstemci işlem ünitesine istenildiğinde TÜBİTAK'ın geliştirdiği ve 2013 yılı başında Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün devreye almayı planladığı akıllı kart uygulamasına uyumlu kart okuyucu takılabilmelidir. Kart okuyucu bu proje kapsamında talep edilmemektedir, sistemin uyumlu olması yeterlidir

2.15. İstemci işlem ünitesinde 10/100/1000 Mbit hız desteği ve PXE & Wake on LAN desteğine sahip en az 1 adet ethernet adaptörü olacaktır.

2.16. İstemci işlem ünitesinde en az 1 adet RS232 portu bulunacaktır.

2.17. İstemci işlem ünitesi üzerinde uyarı sinyali alınabilecek tipte buzzer bulunacaktır.

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

2.19. İstemci işlem ünitesi; şebekedeki voltaj dalgalanmalarına karşı, ürünün stabilitesini ve devamlılığını sağlamak adına voltaj koruma sistemine sahip olacaktır.
2.20. İstemci işlem ünitesi; yetkisiz kişilerce, fiziksel olarak açılmaya karşı korumalı olacaktır. Sistem, yetkisiz kişilerce açılsa dahi kendini bloke edecek ve çalışmasını durduracak şekilde tasarlanmış olacaktır.
2.21. İstemci işlem ünitesi; Elektromanyetik Uyumluluk Yönetmeliği (2004/108/EC) ile uyumlu olup aşağıdaki standartlara uygun olacaktır.
i. EN 55022:2006+A1:2007
ii. EN 55024:1998+A1:2001+A2:2003
iii. EN 61000-3-2:2006+A1:2009+A2:2009
iv. EN 61000-3-3:2008
2.22. İstemci işlem ünitesi; Ekodizayn Yönetmeliği (2009/125/EC) ile uyumlu olup aşağıdaki standartlara uygun olacaktır.
i. EC No 1275/2008
ii. EN 62301:2005
2.23. İstemci işlem ünitesi; CE sertifikasına sahip olacaktır.
2.24. İstemci işlem ünitesi; Medikal Cihazlar Standardına (EN 60601-1) uygun olacaktır.
2.25. İstemci işlem ünitesi; RoHS uyumluluğu olacaktır.
2.26. İstemci işlem ünitesi; WEEE uyumluluğu olacaktır.
2.27. İstemci işlem ünitesi; Energy Star uyumluluğu olacaktır.
2.28. İstemci işlem ünitesi; Avrupa Birliği Veri Koruma Direktifine (95/46/EC) uyumlu olacaktır.
3. Damar izi okuma ünitesi
3.1. Damar İzi Okuma Ünitesi; damar haritasını okuma ve kendi üzerinde AES 256 bit algoritma ve anahtar uzunluğu ile şifreleme özeliklerine sahip olacaktır.
3.2. Damar İzi Okuma Ünitesinden veri çıkışı (Elektronik devreye veya USB arabirimine) tamamen güvenli ve şifreli olmalıdır. Bu verinin tüm arabirimler arası iletiminde veri şifreli olarak taşınmalıdır. Verinin üretilmesi ile veri merkezinde doğrulanmasına kadar her aşama (uçtan uca) güvenli olmalıdır.
3.3. Damar İzi Okuma Ünitesi tekil ve değiştirilemez bir tanımlayıcıya sahip olmalıdır. Bu sayede merkezi olarak onay verilmemiş sistemlerin kullanımı engellenebilmeli ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilmelidir.
3.4. Damar İzi Okuma Ünitesi mümkün olduğunca düzenli temizlik gerektirmemeli, toz, kir, yağ gibi çevresel faktörlerden etkilenmemelidir. Işık altında çalışabilmelidir.
3.5. Damar İzi Okuma Ünitesi; İnsan ağlığına zararlı ürün sınıfında olmamalıdır.
3.6. Damar İzi Okuma Ünitesi'nin FAR (False Acceptance Rate) değeri % 0,00008 ve FRR (False Rejection Rate) değeri % 0,01' den büyük olmamalıdır.
3.7. Damar Okuma Sistemi bahsedilen FAR ve FRR değerlerini tek bir biyometrik okuyucu ve tek bir biyometrik yöntem ile sağlamalıdır. Bu değerler birden fazla biyometrik teknolojinin birleşimi ile sağlanmayacaktır.
3.8. Damar İzi Okuma Ünitesi merkezi olarak (online) 1:1 ve 1:N kimlik doğrulamaya ilave herhangi bir taşıma, depolama materyali olmaksızın imkan sağlamalıdır.

3.9. Damar İzi Okuma Ünitesi, canlı doku tespit (Life Detection) özelliğine sahip olmalıdır.

3.10. Damar İzi Okuma Ünitesi; ağırlığı 50 gr'dan fazla olmamalıdır.

3.11. Damar İzi Okuma Ünitesi; enerjisini istemci ünitesi üzerinden almalı ve maksimum 2.5 Watt enerji tüketimi olmalıdır.

3.12. Damar İzi Okuma Ünitesi'nin çalışma sıcaklık aralığı 0-60 °C olmalıdır.

3.13. Damar izi okuma ünitesi tanımlı olduğu clienttan çıkarılıp başka bir cliente takıldığında çalışmayacaktır.

3.14. Damar İzi Okuma Sensörü boyutları 36x36x28 mm.' den büyük olmamalıdır.
4. Konumlandırma ünitesi
4.1 Konumlandırma Ünitesi; Damar İzi Okuma Ünitesi ile entegre olmalıdır.
4.2 Konumlandırma Ünitesi; her yaş ve eğitim grubundaki insanın rahatlıkla kullanımına imkan verecek, kullanılacak olan uzvun ergonomik yapısına uygun, Damar İzi Okumasını

kolaylaştıran, hata riskini en aza indiren ve Damar İzi Okuma Ünitesi teknik gereksinimlerine uygun tasarımda olacaktır.

5. İstemci giriş-çıkış ünitesi

5.1. İstemci giriş-çıkış ünitesinde en az 3 inch ve 640x480 ekran çözünürlüğünü destekleyen renkli TFT ekran bulunacaktır.

5.2. İstemci giriş-çıkış ünitesinde kullanıcının TC Kimlik bilgisini girmesine olanak tanıyacak 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,*, #, Sil, İptal, Giriş tuşları, 4 adet navigasyon tuşu ve F1, F2, F3, F4 programlanabilir fonksiyon tuşlarını içeren klavye bulunacaktır.

6. İstemci yazılımı

6.1. İstemci yazılımı, Sistemin internete çıkabilmesi için gerekli IP, SubnetMask, Gateway, DNS Server gibi bilgilerin girilmesine imkan sağlayacaktır.

6.2. İstemci yazılımı, Sağlık hizmet sunucularının ID numarasını ve Poliklinik ID'lerinin girilmesine imkan sağlayacaktır.

6.3. İstemci yazılımı, sistemin network ve internete erişebilirliğinin tespit edilmesi için kullanımı kolay network tanımlama araçlarına sahip olacaktır

6.4. İstemci yazılımı, merkezi sistem üzerinden istenildiği zaman güncellenebilmelidir.

6.5. İstemci yazılımı, üzerinde çalışan işletim sistemi ile ilgili güncellemeler merkez tarafından yayınlandığı takdirde, merkezden gerekli verileri güvenli ortamda kendi üzerine çekebilmeli, yazılım güncellemelerini kullanıcı müdahalesine gerek kalmadan yapmalıdır.

6.6. İstemci yazılımı, KeyPad'den girilen komutları göre biyometrik doğrulama ve biyometrik kayıt işlemlerini gerçekleştirecek, işlem adımlarını operatörün, üzerindeki ekrandan takip etmesini sağlayacak, biyometrik görüntünün alınması sırasında görüntülü yönlendirme yapacak şekilde tasarlanmalıdır.

6.7. İstemci yazılımı, sunucu yazılımı ile Secure Socket Layer üzerinden ve en az 128 bit anahtar uzunluğu kullanılarak iletişime geçecektir.

6.8. İstemci yazılımı, güvenlik sebebi ile; biyometrik bilgileri, biyometrik sensörün 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 şifrelemelidir.

6.9. İstemci yazılımı, güvenlik sebebi ile okuyucu sensör ile istemci cihazı arasındaki biyometrik veri 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 şifreleyip ve iletilebilmelidir.

6.10. Okuyucu sensör, okuma işleminin hemen ardından, biyometrik veri istemci cihaza gönderilmeden biyometrik bilgileri geri dönüşümsüz bir algoritmadan geçirecek, orijinal biyometrik görüntüyü tutmayacak ve daha sonra istemci cihazına biyometrik bilgi iletilecektir. Algoritmadan geçirilen veriden orijinal biyometrik imaja dönülmesi mümkün olmayacaktır.

6.11. İstemci yazılımı, ilk kayıt ve ilk doğrulama esnasında alınan ve doğrulanan kaydın kalitesini değerlendirebilecek, alınan biyometrik veri kalitesi yeterli değil ise, biyometrik kaydın merkeze gönderilmeden önce yenilenebilmesine imkan sağlayacaktır.

6.12. İstemci yazılımı, belirlenecek özel durumların merkeze bildirilebilmesine imkan sağlayacak altyapıda olacaktır. (Örneğin hastanın bir elinin olmaması gibi.)

6.13. İstemci yazılımı, hastalara ait TC Kimlik numaralarının hatalı girilmesini engelleyecek yazılımsal kontrollere sahip olmalıdır.

6.14. İstemci yazılımı, ilk kurulum işlemi sırasında ve hastane, poliklinik bilgilerinin değiştirilmesi durumunda merkez ile iletişime geçip, aktivasyon işlemi yapılmadan kayıt doğrulama işlemi yapılmasına imkan vermeyecektir.

6.15. İstemci yazılımı, üzerinde oluşabilecek problemlere karşı, üzerinde tuttuğu hata ve sistem loglarını merkeze gönderebilecek özelliğe sahip olmalıdır.

6.16. İstemci sistemi ve yazılımı üzerinde kesinlikle kalıcı olarak biyometrik veri bulundurulmayacak ve işlenmeyecektir. İlk kayıt veya doğrulama amaçlı biyometrik veri alınır alınmaz güvenli bir şekilde merkezi sunucu yazılımına iletilecektir. Biyometrik verinin doğru olup olmadığına karar verme işlemi merkezi sunucu yazılımı üzerinde güvenli ortamda yapılacak, istemci yazılımına sadece onay bilgisi gönderilecektir.

6.17. İstemci yazılımı ve istemcinin çalışması için herhangi bir başka bilgisayar ve yazılıma gerek duyulmayacak, sistem kendi başına stand-alone çalışabilecek yapıda olmalıdır.

EK 1- (2-A)

2.TİP BİYOMETRİK KİMLİK DOĞRULAMA SİSTEMİ SEÇENEĞİ

(2-A)- Parmak Damar İzi Sistemi Biyometrik Kimlik Doğrulama Ünitesinin Bileşenleri

1. İstemci Donanımı Bakım ve Kurulumu

1.1. Cihaz ile birlikte çalışması için gerekli tüm çevre-birimler/donanım teslim edilecektir.
1.2. Altyapı ve kablolama ürünü satın alan SHS'ler tarafından hazırlanmış olacaktır.
1.3. Cihaz devreye alınması sırasında gerekli olacak tüm bilgiler SHS tarafından belirlenmiş olan kurulum sorumlusuna iletilecektir.
1.4. Cihaz arızaları için donanım değişimi yapılarak çözüm sağlanacaktır.
1.5. Cihazın; yazılım güncellemelerini merkezi, otomatik ve güvenli şekilde yapılabilmesi sağlanmalıdır.
1.6. Cihazların merkezi sistem ile takip edilebilmesi sağlanmalıdır.
1.7. Cihazda oluşacak sorunlar için kolay, anlaşılır ve görüntülenebilir hata kodları üretilmesi sağlanmalıdır.
1.8. Cihaz sorunları için uzaktan destek verilmesine olanak sağlanmalıdır.
1.9. Cihaz ilk kurulum/devreye alınma hizmeti standart olarak verilmelidir.
1.10. Cihazın fiziksel sorunlarından dolayı değişimi en fazla 5 iş gününde sağlanmalıdır.
1.11. Cihaz 2 yıl standart garanti ile satışı yapılacak olup, 10 yıl yedek parça sağlanmalıdır.
1.12. Cihazlar, sevk esnasında sigortalı olarak taşınmalıdır.

2. İstemci Biyometrik Kimlik Doğrulama Ünitesi

2.1. İstemci işlem ünitesi; 7 gün 24 saat esasına göre ve 0°C ila 60°C sıcaklık aralığında kesintisiz olarak çalışabilecektir.
2.2. İstemci işlem ünitesi üzerinde fan bulunmayacaktır.
2.3. İstemci işlem ünitesi; harici olarak farklı cihazlar ile boot edilemeyecektir.
2.4. İstemci işlem ünitesine harici olarak başka bir depolama aygıtı bağlanması durumunda, bu aygıta sistem üzerinden herhangi bilgi depolanması mümkün olmayacaktır.
2.5. İstemci işlem ünitesi, kişinin TC Kimlik No ve Biyometrik Kimlik bilgilerini kriptolayarak ana sunucuya transfer edecek teknolojiye sahip olacaktır.
2.6. İstemci işlem ünitesi sadece tek bir Damar İzi Okuma Ünitesi bağlantısına izin verecektir
2.7. İstemci işlem ünitesine istenildiğinde TÜBİTAK'ın geliştirdiği akıllı kart uygulamasına uyumlu kart okuyucu takılabilmelidir. Kart okuyucu bu proje kapsamında talep edilmemektedir, sistemin uyumlu olması yeterlidir
2.8. İstemci işlem ünitesinde 10/100/1000Mbit hız desteği ve PXE & Wake on LAN desteğine sahip en az 1 adet ethernet adaptörü olacaktır.
2.9. İstemci işlem ünitesi; şebekedeki voltaj dalgalanmalarına karşı, ürünün stabilitesini ve devamlılığını sağlamak adına voltaj koruma sistemine sahip olacaktır.
2.10. İstemci işlem ünitesi; yetkisiz kişilerce, fiziksel olarak açılmaya karşı korumalı olacaktır. Sistem, yetkisiz kişilerce açılsa dahi kendini bloke edecek ve çalışmasını durduracak şekilde tasarlanmış olacaktır.
2.11. İstemci işlem ünitesi; İnsan sağlığını tehlikeye sokacak herhangi bir ürün grubunda olmamalıdır ve herhangi bir zararlı madde içermemelidir.
2.12. İstemci işlem ünitesi Elektromanyetik Uyumluluk Yönetmeliği (2004/108/EC) ile uyumlu olup en az aşağıdaki standartlara uygun olacaktır
2.13. EN 55022: 2006 +A1: 2007
2.14. EN 61000-3-2: 2006+A1: 2009+A2:2009; EN 61000-3-3; 2008
2.15. EN 55024: 1998+A1: 2001+A2: 2003
2.16. IEC 61000-4-2: 2009, IEC 61000-4-3: 2006
2.17. IEC 61000-4-4: 2004+A1: 2010, IEC 61000-4-5: 2006
2.18. IEC 61000-4-6: 2009
2.19. IEC 61000-4-8: 2005, IEC 61000-4-11: 2004
2.20. İstemci işlem ünitesi CE ve RoHS sertifikasına sahip olacaktır.

2.21. İstemci işlem ünitesi, tekil ve değiştirilemez bir tanımlayıcıya sahip olacaktır. Bu sayede merkezi olarak onay verilmemiş sistemlerin kullanımı engellenebilecek ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilecektir.
2.22. İstemci işlem ünitesi üzerinde kullanıcının TC Kimlik bilgisini girmesine olanak tanıyacak 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, Sil, İptal, Giriş tuşlarının yer aldığı dokunmatik ekran, ve F1, F2, F3, F4 programlanabilir fonksiyon tuşlarını içeren tuşlar bulunacaktır. Cihaz ayrıca bir klavyeye ihtiyaç duymayacaktır.

3. Damar İzi Okuyucu

3.1. Damar izi okuyucu damar haritasını okuma ve aktarmadan önce kendi üzerinde en az AES 256 bit algoritma ve anahtar uzunluğu ile şifreleme özeliklerine sahip olacaktır.
3.2. Damar izi okuyucudan veri çıkışı (Elektronik devreye veya USB arabirimine) tamamen güvenli ve şifreli olmalıdır. Bu verinin tüm arabirimler arası iletiminde veri şifreli olarak taşınmalıdır. Verinin üretilmesi ile doğrulanmasına kadar her aşama (uçtan uca) güvenli olmalıdır.
3.3. Damar izi okuyucu, olarak (online) 1:1 ve 1:N kimlik doğrulamaya ilave herhangi bir taşıma, depolama materyali olmaksızın doğrulamaya imkan sağlamalıdır. Damar izi okuyucu üzerinde okunan biyometrik veri ile ilgili hiç bir kayıt yapılmayacak, okunan verileri kayıt edilmesi engellenmiş olacaktır.
3.4. Damar izi okuyucunun FAR değeri % 0.0001 ve FRR değeri %0,01 en büyük olmayacaktır.
3.5. Damar izi okuyucu, FAR ve FRR değerlerini tek bir biyometrik okuyucu ve tek bir biyometrik yöntem ile sağlamalıdır.
3.6. Damar İzi okuyucu, insan sağlığına zararlı ürün sınıfında olmamalıdır.
3.7. Damar izi okuyucu, canlı doku tespit (Life Detection) özelliğine sahip olmalıdır.
3.8. Damar izi okuyucunun çalışma sıcaklığı en az 0 °C ile 60 °C aralığında olmalıdır. Damar izi okuyucu, tekil ve değiştirilemez bir tanımlayıcıya sahip olmalıdır. Bu sayede merkezi olarak onay verilmemiş okuyucuların kullanımı engellenebilmeli ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilmelidir.

4. İstemci Ünitesi Yazılmı

4.1. İstemci yazılımı, Sistemin internete çıkabilmesi için gerekli IP, SubnetMask, Gateway, DNS Server gibi bilgilerin girilmesine imkan sağlayacaktır.
4.2. İstemci yazılımı, SHS'larının ID numarasının ve Poliklinik ID'lerinin girilmesine imkan sağlayacaktır.
4.3. İstemci yazılımı, sistemin network ve internete erişebilirliğinin tespit edilmesi için kullanımı kolay network tanımlama araçlarına sahip olacaktır
4.4. İstemci yazılımı, merkezi sistem üzerinden istenildiği zaman güncellenebilmelidir.
4.5. İstemci yazılımı, üzerinde çalışan işletim sistemi ile ilgili güncellemeler merkez tarafından yayınlandığı taktirde, merkezden gerekli verileri güvenli ortamda kendi üzerine çekebilmeli, yazılım güncellemelerini kullanıcı müdahalesine gerek kalmadan yapmalıdır.
4.6. İstemci yazılımı girilen komutlara göre biyometrik doğrulama ve biyometrik kayıt işlemlerini gerçekleştirecek, işlem adımlarını operatörün, üzerindeki ekrandan takip etmesini sağlayacak, biyometrik görüntünün alınması sırasında görüntülü yönlendirme yapacak şekilde tasarlanmalıdır.
4.7. İstemci yazılımı, sunucu yazılımı ile Secure Socket Layer üzerinden ve en az 128 bit anahtar uzunluğu kullanılarak iletişime geçecektir.
4.8. İstemci yazılımı, güvenlik sebebi ile; biyometrik bilgileri, biyometrik sensörün 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 şifrelemelidir.
4.9. İstemci yazılımı, güvenlik sebebi ile okuyucu sensör ile istemci cihazı arasındaki biyometrik veri 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 şifreleyip ve iletilebilmelidir.
4.10. Okuyucu sensör, okuma işleminin hemen ardından, biyometrik veri istemci cihaza gönderilmeden biyometrik bilgileri geri dönüşümsüz bir algoritmadan geçirecek, orijinal biyometrik görüntüyü tutmayacak ve daha sonra istemci cihazına biyometrik bilgi iletilecektir. algoritmadan geçirilen veriden orijinal biyometrik imaja dönülmesi mümkün olmayacaktır.

4.11. İstemci yazılımı, belirlenecek özel durumların merkeze bildirilebilmesine imkan sağlayacak altyapıda olacaktır. (Örneğin hastanın uygun eli veya parmağının olmaması gibi.)
4.12. İstemci yazılımı, hastalara ait TC Kimlik numaralarının hatalı girilmesini engelleyecek yazılımsal kontrollere sahip olmalıdır. İstemci yazılımı, ilk kurulum işlemi sırasında ve hastane, poliklinik bilgilerinin değiştirilmesi durumunda merkez ile iletişime geçip, aktivasyon işlemi yapılmadan kayıt doğrulama işlemi yapılmasına imkan vermeyecektir.
4.13. İstemci yazılımı, üzerinde oluşabilecek problemlere karşı, üzerinde tuttuğu hata ve sistem loglarını merkeze gönderebilecek özelliğe sahip olmalıdır.
4.14. İstemci sistemi ve yazılımı üzerinde kesinlikle kalıcı olarak biyometrik veri bulundurulmayacak ve işlenmeyecektir
4.15. İstemci yazılımı ve istemcinin çalışması için herhangi bir başka bilgisayar ve yazılıma gerek duyulmayacak, sistem kendi başına stand-alone çalışacak yapıda olmalıdır.
4.16. Veri merkezi ve sağlık sunucularında konumlandırılan(Uçtan uca) tüm cihazların güvenliği Tübitak tarafından incelenecek olup herhangi bir güvenlik eksiği olması durumunda Yüklenici tüm ürünleri için hiçbir hak iddia etmeden cihazlar ve yazılımlar üzerinde gerekli değişiklikleri yapacaktır
4.17. BKDÜ cihazlarının teknik özellikleri kurumun mevcut altyapısında bulunan diğer biyometrik teknolojilerinden daha düşük özellikte olmayacaktır.
4.18. Veri merkezinde konumlandırılan cihazların sistemin çalışması noktasındaki performansı kurumun mevcut altyapısında bulunan diğer biyometrik teknolojilerin performansından düşük olamaz. Sistemin performansının eksik olduğu düşünüldüğü durumda veri merkezine yeni ürünler eklenecektir.

EK 1-(2-B)

2.TİP BİYOMETRİK KİMLİK DOĞRULAMA SİSTEMİ SEÇENEĞİ

(2-B)- Parmak Damar İzi Sistemi Biyometrik Kimlik Doğrulama Ünitesinin Bileşenleri

1. İstemci Donanımı Bakım ve Kurulumu

1.1. Cihaz ile birlikte çalışması için gerekli tüm çevre-birimler/donanım teslim edilecektir.
1.2. Altyapı ve kablolama ürünü satın alan SHS'ler tarafından hazırlanmış olacaktır.
1.3. Cihaz devreye alınması sırasında gerekli olacak tüm bilgiler SHS tarafından belirlenmiş olan kurulum sorumlusuna iletilecektir.
1.4. Cihaz arızaları için donanım değişimi yapılarak çözüm sağlanacaktır.
1.5. Cihazın; yazılım güncellemelerini merkezi, otomatik ve güvenli şekilde yapılabilmesi sağlanmalıdır.
1.6. Cihazların merkezi sistem ile takip edilebilmesi sağlanmalıdır.
1.7. Cihazda oluşacak sorunlar için kolay, anlaşılır ve görüntülenebilir hata kodları üretilmesi sağlanmalıdır.
1.8. Cihaz sorunları için uzaktan destek verilmesine olanak sağlanmalıdır.
1.9. Cihaz ilk kurulum/devreye alınma hizmeti standart olarak verilmelidir.
1.10. Cihazın fiziksel sorunlarından dolayı değişimi en fazla 5 iş gününde sağlanmalıdır.
1.11. Cihaz 2 yıl standart garanti ile satışı yapılacak olup, 10 yıl yedek parça sağlanmalıdır.
1.12. Cihazlar, sevk esnasında sigortalı olarak taşınmalıdır.

2. İstemci Biyometrik Kimlik Doğrulama Ünitesi

2.1. İstemci işlem ünitesi; 7 gün 24 saat esasına göre ve en az 0-60° C sıcaklık aralığında ve %20-80 nem oranında kesintisiz olarak çalışabilecektir.
2.2. İstemci işlem ünitesi üzerinde fan bulunmayacaktır.
2.3. İstemci işlem ünitesi; harici olarak farklı cihazlar ile boot edilemeyecektir.
2.4. İstemci işlem ünitesine harici olarak başka bir depolama aygıtı bağlanması durumunda, bu aygıta sistem üzerinden herhangi bilgi depolanması mümkün olmayacaktır.
2.5. İstemci işlem ünitesi, kişinin TC Kimlik No Biyometrik Kimlik bilgilerini kriptolayarak ana sunucuya transfer edecek teknolojiye sahip olacaktır.
2.6. İstemci işlem ünitesi sadece tek bir Damar İzi Okuma Ünitesi bağlantısına izin verecektir
2.7. İstemci işlem ünitesine istenildiğinde TÜBİTAK'ın geliştirdiği akıllı kart uygulamasına uyumlu kart okuyucu takılabilmelidir. Kart okuyucu bu proje kapsamında talep edilmemektedir, sistemin uyumlu olması yeterlidir
2.8. İstemci işlem ünitesi en az 600dpi çözünürlükte veri alabilmelidir. İstemci İşlem Ünitesinde 10/100/1000 Mbit hız desteği ve PXE & Wake on LAN desteğine sahip en az 1 adet Ethernet adaptörü olacaktır.
2.9. İstemci işlem ünitesi; şebekedeki voltaj dalgalanmalarına karşı, ürünün stabilitesini ve devamlılığını sağlamak adına voltaj koruma sistemine sahip olacaktır.
2.10. İstemci işlem ünitesi; yetkisiz kişilerce, fiziksel olarak açılmaya karşı korumalı olacaktır. Sistem, yetkisiz kişilerce açılsa dahi kendini bloke edecek ve çalışmasını durduracak şekilde tasarlanmış olacaktır.
2.11. İstemci işlem ünitesi; parmak damarını kullanarak, kişi tespitinde tekillik başarısını NIST sonuçlarına göre sağlamalıdır. İstemci İşlem Ünitesi; Elektromanyetik Uyumluluk Yönetmeliği (2004/108/EC) ile uyumlu olup aşağıdaki standartlara uygun olacaktır.
2.12. İstemci işlem ünitesi, insan sağlığını tehlikeye sokacak herhangi bir ürün grubunda olmamalıdır ve herhangi bir zararlı madde içermemelidir.
2.13. EN 55022: 2006 +A1: 2007
2.14. EN 61000-3-2: 2006+A1: 2009+A2:2009; EN 61000-3-3; 2008
2.15. EN 55024: 1998+A1: 2001+A2: 2003
2.16. IEC 61000-4-2: 2009, IEC 61000-4-3: 2006
2.17. IEC 61000-4-4: 2004+A1: 2010, IEC 61000-4-5: 2006
2.18. IEC 61000-4-6: 2009
2.19. IEC 61000-4-8: 2005, IEC 61000-4-11: 2004

2.20. İstemci işlem ünitesi CE, FCC, UL/CUL, BSMI, VCCI ve WEEE belgelerine sahip olması, standartlarını sağlaması ve incelemeleri yapılmış olması gerekmektedir. İstemci İşlem Ünitesi CE ve RoHS sertifikalarına sahip olacaktır.
2.21. İstemci işlem ünitesi, tekil ve değiştirilemez bir tanımlayıcıya sahip olacaktır. Bu sayede merkezi olarak onay verilmemiş sistemlerin kullanımı engellenebilecek ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilecektir.
2.22. İstemci işlem ünitesi 1-1 ve 1-N eşleme işleminde kullanılabilmelidir. İstemci işlem Ünitesi üzerinde kullanıcının TC Kimlik bilgisini girmesine olanak tanıyacak 0,1,2,3,4,5,6,7,8,9, Sil, İptal, Giriş tuşlarının yer aldığı manuel yahut dokunmatik ekran ve F1,F2,F3,F4 programlanabilir fonksiyon tuşlarını içeren tuşlar bulunacaktır. Cihaz ayrıca bir klavyeye ihtiyaç duymayacaktır.

3. Damar İzi Okuyucu

3.1. Damar izi okuyucu damar haritasını okuma ve aktarmadan önce kendi üzerinde en az AES 256 bit algoritma ve anahtar uzunluğu ile şifreleme özeliklerine sahip olacaktır.
3.2. Damar izi okuyucudan veri çıkışı (Elektronik devreye veya USB arabirimine) tamamen güvenli ve şifreli olmalıdır. Bu verinin tüm arabirimler arası iletiminde veri şifreli olarak taşınmalıdır. Verinin üretilmesi ile doğrulanmasına kadar her aşama (uçtan uca) güvenli olmalıdır.
3.3. Damar izi okuyucu, olarak (online) 1:1 ve 1:N kimlik doğrulamaya ilave herhangi bir taşıma, depolama materyali olmaksızın doğrulamaya imkan sağlamalıdır. Damar izi okuyucu üzerinde okunan biyometrik veri ile ilgili hiç bir kayıt yapılmayacak, okunan verileri kayıt edilmesi engellenmiş olacaktır.
3.4. Damar izi okuyucunun FAR değeri % 0.0001 ve FRR değeri % 0,01 en büyük olmayacaktır.
3.5. Damar izi okuyucu, FAR ve FRR değerlerini tek bir biyometrik cihaz okuyucu yöntem ile sağlamalıdır.
3.6. Damar İzi okuyucu, insan sağlığına zararlı ürün sınıfında olmamalıdır.
3.7. Damar izi okuyucu, canlı doku tespit (Life Detection) özelliğine sahip olmalıdır.
3.8. Damar izi okuyucunun çalışma sıcaklığı en az 0 °C ile 60 °C aralığında olmalıdır. Damar izi okuyucu, tekil ve değiştirilemez bir tanımlayıcıya sahip olmalıdır. Bu sayede merkezi olarak onay verilmemiş okuyucuların kullanımı engellenebilmeli ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilmelidir.

4. İstemci Ünitesi Yazılımı

4.1. İstemci yazılımı kullanıcı girişi, yönetici girişi, kayıt ve doğrulama gibi aşamalar öncesi tanımlı ID erişimini sağlamak için gerekli arayüz tasarımına sahip olacaktır. İstemci yazılımı, sistemin internete çıkabilmesi için gerekli IP, SubnetMask, Gateway, DNS Server gibi bilgilerin girilmesine imkan sağlayacaktır.
4.2. İstemci yazılımı, SHS'larının ID numarasının ve Poliklinik ID'lerinin girilmesine imkan sağlayacaktır.
4.3. İstemci yazılımı, sistemin network ve internete erişebilirliğinin tespit edilmesi için kullanımı kolay network tanımlama araçlarına sahip olacaktır
4.4. İstemci yazılımı, merkezi sistem üzerinden istenildiği zaman güncellenebilmelidir.
4.5. İstemci yazılımı, üzerinde çalışan işletim sistemi ile ilgili güncellemeler merkez tarafından yayınlandığı taktirde, merkezden gerekli verileri güvenli ortamda kendi üzerine çekebilmeli, yazılım güncellemelerini kullanıcı müdahalesine gerek kalmadan yapmalıdır.
4.6. İstemci yazılımı girilen komutlara göre biyometrik doğrulama ve biyometrik kayıt işlemlerini gerçekleştirecek, işlem adımlarını operatörün, üzerindeki ekrandan takip etmesini sağlayacak, biyometrik görüntünün alınması sırasında görüntülü yönlendirme yapacak şekilde tasarlanmalıdır.
4.7. İstemci yazılımı merkez sunuculara erişimi sağlamak üzere gerekli adreslerin belirtilmesine imkân veren tanımlanmış alanlara sahip olacaktır. İstemci yazılımı, sunucu yazılımı ile Secure Socket Layer üzerinden ve en az 128 bit anahtar uzunluğu kullanılarak iletişime geçecektir.
4.8. İstemci yazılımı, güvenlik sebebi ile; biyometrik bilgileri, biyometrik sensörün 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 şifrelemelidir.
4.9. İstemci yazılımı, güvenlik sebebi ile okuyucu sensör ile istemci cihazı arasındaki biyometrik veri 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 şifreleyip ve iletilebilmelidir.
4.10. Okuyucu sensör, okuma işleminin hemen ardından, biyometrik veri istemci cihaza gönderilmeden biyometrik bilgileri geri dönüşümsüz bir algoritmadan geçirecek, orijinal biyometrik görüntüyü tutmayacak ve daha sonra istemci cihazına biyometrik bilgi iletilecektir. Algoritmadan geçirilen veriden orijinal biyometrik imaja dönülmesi mümkün olmayacaktır.
4.11. İstemci yazılımı, belirlenecek özel durumların merkeze bildirilebilmesine imkan sağlayacak altyapıda olacaktır. (Örneğin hastanın uygun eli veya parmağının olmaması gibi.)
4.12. İstemci yazılımı, hastalara ait TC Kimlik numaralarının hatalı girilmesini engelleyecek yazılımsal kontrollere sahip olmalıdır. İstemci yazılımı, ilk kurulum işlemi sırasında ve hastane, poliklinik bilgilerinin değiştirilmesi durumunda merkez ile iletişime geçip, aktivasyon işlemi yapılmadan kayıt doğrulama işlemi yapılmasına imkan vermeyecektir.
4.13. İstemci yazılımı, üzerinde oluşabilecek problemlere karşı, üzerinde tuttuğu hata ve sistem loglarını merkeze gönderebilecek özelliğe sahip olmalıdır.
4.14. İstemci sistemi ve yazılımı üzerinde kesinlikle kalıcı olarak biyometrik veri bulundurulmayacak ve işlenmeyecektir
4.15. İstemci yazılım mimarisi ilişkilendirilmiş süreçlerin akış çizelgeleri doğrultusunda kullanıcıyı yönlendirecek yapıya sahip olacaktır. İstemci yazılımı ve istemcinin çalışması için herhangi bir başka bilgisayar ve yazılıma gerek duyulmayacak, sistem kendi başına stand-alone çalışacak yapıda olmalıdır.
4.16. İstemci tanımlı iş süreçlerinin kullanıcı tarafından hatasız sürdürülmesini sağlayacak yardımcı tetik mekanizmaları, uyarı alanları, sıralı iş adımları gibi özel yapılara sahip olacaktır.
4.17. İstemci yazılımı yetkili ID erişimi ile yetki sınıflarına göre kullanıcı grup ayrımını yapabilecek ve her kullanıcıya ilişkili olduğu süreçler içerisinde hareket imkânı sağlayacak tasarıma sahip olacaktır.
4.18. İstemci yazılımı merkez birimler üzerinden kullanıcı bağımsız şekilde kendini güncelleyebilecek yapıda olacaktır.
4.19. Güncelleme işlemleri son güncel sürümün temini aşamasından önce istemci yazılımı üzerinden yapılan ilk yetkili kullanıcı erişimi ile başlayacak ve her hangi bir dış müdahale olmadan sonlandırılarak yeniden erişim talebi sonucu tamamlanacak yapıda olacaktır.
4.20. İstemci yazılımı arayüzleri yetkili kullanıcının gerçekleştireceği yeni kayıt işlemi esnasında kullanıcı ve biyometrik veri sahibini yönlendirecek şekilde görsel öğelerle desteklenmiş olacaktır.
4.21. İstemci yazılımı işlenen biyometrik verinin işlevsellik açısından kalitesini belirleyebilecek ve yetersiz bulunan verinin yeniden talebini sağlayan uyarı mekanizmalarına sahip olacaktır.
4.22. İstemci yazılımı gerçekleştirilen tanımlı eylemlerin tamamını kullanıcı, zaman, bağlı bulunan kurum kuruluş, veri bilgisi, vb. alanları da dikkate alarak LOG kayıtları oluşturmak sureti ile merkez birimlere aktarabilecek yapıda olacaktır.
4.23. İstemci yazılımı biyometrik veri temini ve merkez sunucular ile yürütülen tüm faaliyetler için her hangi bir ek yazılım aracına ihtiyaç duymadan çalışabilecek mimaride olacaktır.
4.24. Veri merkezi ve sağlık sunucularında konumlandırılan(Uçtan uca) tüm cihazların güvenliği Tübitak tarafından incelenecek olup herhangi bir güvenlik eksiği olması durumunda Yüklenici tüm ürünleri için hiçbir hak iddia etmeden cihazlar ve yazılımlar üzerinde gerekli değişiklikleri yapacaktır.
4.25. Veri merkezinde konumlandırılan cihazların sistemin çalışması noktasındaki performansı kurumun mevcut altyapısında bulunan diğer biyometrik teknolojilerin performansından düşük olamaz. Sistemin performansının eksik olduğu düşünüldüğü durumda veri merkezine yeni ürünler eklenecek ve ihtiyaca göre revize edilecektir.
4.26. BKDÜ cihazlarının teknik özellikleri kurumun mevcut altyapısında bulunan diğer biyometrik teknolojilerinden daha düşük özellikte olmayacaktır.

EK 1-(2-C)

2.TİP BİYOMETRİK KİMLİK DOĞRULAMA SİSTEMİ SEÇENEĞİ

(2-C)- Parmak Damar İzi Sistemi Biyometrik Kimlik Doğrulama Ünitesinin Bileşenleri

1. İstemci Donanımı Bakım ve Kurulumu

1.1. Cihaz ile birlikte çalışması için gerekli tüm çevre-birimler/donanım teslim edilecektir.
1.2. Altyapı ve kablolama ürünü satın alan SHS'ler tarafından hazırlanmış olacaktır.
1.3. Cihaz devreye alınması sırasında gerekli olacak tüm bilgiler SHS tarafından belirlenmiş olan kurulum sorumlusuna iletilecektir.
1.4. Cihaz arızaları için donanım değişimi yapılarak çözüm sağlanacaktır.
1.5. Cihazın; yazılım güncellemelerini merkezi, otomatik ve güvenli şekilde yapılabilmesi sağlanmalıdır.
1.6. Cihazların merkezi sistem ile takip edilebilmesi sağlanmalıdır.
1.7. Cihazda oluşacak sorunlar için kolay, anlaşılır ve görüntülenebilir hata kodları üretilmesi sağlanmalıdır.
1.8. Cihaz sorunları için uzaktan destek verilmesine olanak sağlanmalıdır.
1.9. Cihaz ilk kurulum/devreye alınma hizmeti standart olarak verilmelidir.
1.10. Cihazın fiziksel sorunlarından dolayı değişimi en fazla 5 iş gününde sağlanmalıdır.
1.11. Cihaz 2 yıl standart garanti ile satışı yapılacak olup, 10 yıl yedek parça sağlanmalıdır.
1.12. Cihazlar, sevk esnasında sigortalı olarak taşınmalıdır.

2. İstemci Biyometrik Kimlik Doğrulama Ünitesi

2.1. İstemci işlem ünitesi; 7 gün 24 saat esasına göre ve 0°C ila 60°C sıcaklık aralığında kesintisiz olarak çalışabilecektir.
2.2. İstemci işlem ünitesi üzerinde fan bulunmayacaktır.
2.3. İstemci işlem ünitesi; harici olarak farklı cihazlar ile boot edilemeyecektir.
2.4. İstemci işlem ünitesine harici olarak başka bir depolama aygıtı bağlanması durumunda, bu aygıta sistem üzerinden herhangi bilgi depolanması mümkün olmayacaktır.
2.5. İstemci işlem ünitesi, kişinin TC Kimlik No ve Biyometrik Kimlik bilgilerini kriptolayarak ana sunucuya transfer edecek teknolojiye sahip olacaktır.
2.6. İstemci işlem ünitesi sadece tek bir Damar İzi Okuma Ünitesi bağlantısına izin verecektir
2.7. İstemci işlem ünitesine istenildiğinde TÜBİTAK'ın geliştirdiği akıllı kart uygulamasına uyumlu kart okuyucu takılabilmelidir. Kart okuyucu bu proje kapsamında talep edilmemektedir, sistemin uyumlu olması yeterlidir
2.8. İstemci işlem ünitesinde 10/100/1000 Mbit hız desteği ve PXE & Wake on LAN desteğine sahip en az 1 adet ethernet adaptörü olacaktır. SHS'nin isteği doğrultusunda wireless (kablosuz) modülü opsiyonel olarak eklenebilir yapıda olacaktır.
2.9. İstemci işlem ünitesi; şebekedeki voltaj dalgalanmalarına karşı, ürünün stabilitesini ve devamlılığını sağlamak adına voltaj koruma sistemine sahip olacaktır.
2.10. İstemci işlem ünitesi; Yetkisiz kişilerce, fiziksel olarak açılmaya karşı korumalı olacaktır. Sistem, yetkisiz kişilerce açılsa dahi kendini bloke edecek ve çalışmasını durduracak şekilde tasarlanmış olacaktır.
2.11. İstemci işlem ünitesi; İnsan sağlığını tehlikeye sokacak herhangi bir ürün grubunda olmamalıdır ve herhangi bir zararlı madde içermemelidir.
2.12. İstemci işlem ünitesi; Elektromanyetik Uyumluluk Yönetmeliği (2004/108/EC) ile uyumlu olup aşağıdaki standartlara uygun olacaktır.
2.13. EN 55022: 2006 +A1: 2007
2.14. EN 61000-3-2: 2006+A1: 2009+A2:2009; EN 61000-3-3; 2008
2.15. EN 55024: 1998+A1: 2001+A2: 2003
2.16. IEC 61000-4-2: 2009, IEC 61000-4-3: 2006
2.17. IEC 61000-4-4: 2004+A1: 2010, IEC 61000-4-5: 2006
2.18. IEC 61000-4-6: 2009
2.19. IEC 61000-4-8: 2005, IEC 61000-4-11: 2004
2.20. İstemci işlem ünitesi CE ve RoHS sertifikasına sahip olacaktır.

2.21. İstemci işlem ünitesi, tekil ve değiştirilemez bir tanımlayıcıya sahip olacaktır. Bu sayede merkezi olarak onay verilmemiş sistemlerin kullanımı engellenebilecek ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilecektir.
2.22. İstemci işlem ünitesi üzerinde kullanıcının TC Kimlik bilgisini girmesine olanak tanıyacak 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, İptal, Giriş tuşlarının yer aldığı ve dört adet naviasyon programlanabilir fonksiyon tuşlarını içeren tuşlar bulunacaktır. Cihaz ayrıca bir klavyeye ihtiyaç duymayacaktır.

3. Damar İzi Okuyucu

3.1. Damar izi okuyucu damar haritasını okuma ve aktarmadan önce kendi üzerinde en az AES 256 bit algoritma ve anahtar uzunluğu ile şifreleme özeliklerine sahip olacaktır.
3.2. Damar izi okuyucudan veri çıkışı (Elektronik devreye veya USB arabirimine) tamamen güvenli ve şifreli olmalıdır. Bu verinin tüm arabirimler arası iletiminde veri şifreli olarak taşınmalıdır. Verinin üretilmesi ile doğrulanmasına kadar her aşama (uçtan uca) güvenli olmalıdır.
3.3. Damar izi okuyucu, olarak(online) 1:1 ve 1:N kimlik doğrulamaya ilave herhangi bir taşıma, depolama materyali olmaksızın doğrulamaya imkan sağlamalıdır. Damar izi okuyucu üzerinde okunan biyometrik veri ile ilgili hiç bir kayıt yapılmayacak, okunan verileri kayıt edilmesi engellenmiş olacaktır.
3.4. Damar izi okuyucunun FAR değeri % 0.0001 ve FRR değeri %0,01 den büyük olmayacaktır.
3.5. Damar izi okuyucu, FAR ve FRR değerlerini tek bir biyometrik okuyucu ve tek bir biyometrik yöntem ile sağlamalıdır.
3.6. Damar İzi okuyucu, insan sağlığına zararlı ürün sınıfında olmamalıdır.
3.7. Damar izi okuyucu, canlı doku tespit (Life Detection) özelliğine sahip olmalıdır.
3.8. Damar izi okuyucunun çalışma sıcaklığı en az 0 °C ile 60 °C aralığında olmalıdır. Damar izi okuyucu, tekil ve değiştirilemez bir tanımlayıcıya sahip olmalıdır. Bu sayede merkezi olarak onay verilmemiş okuyucuların kullanımı engellenebilmeli ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilmelidir.

4. İstemci Ünitesi Yazılımı

4.1. İstemci yazılımı, Sistemin internete çıkabilmesi için gerekli IP, SubnetMask, Gateway, DNS Server gibi bilgilerin girilmesine imkan sağlayacaktır.
4.2. İstemci yazılımı, SHS'larının ID numarasının ve Poliklinik ID'lerinin girilmesine imkan sağlayacaktır.
4.3. İstemci yazılımı, sistemin network ve internete erişebilirliğinin tespit edilmesi için kullanımı kolay network tanımlama araçlarına sahip olacaktır. Yazılım ayrıca kablosuz internet erişimine destek sağlayabilir yapıda olacaktır.
4.4. İstemci yazılımı, merkezi sistem üzerinden istenildiği zaman güncellenebilmelidir.
4.5. İstemci yazılımı, üzerinde çalışan işletim sistemi ile ilgili güncellemeler merkez tarafından yayınlandığı taktirde, merkezden gerekli verileri güvenli ortamda kendi üzerine çekebilmeli, yazılım güncellemelerini kullanıcı müdahalesine gerek kalmadan yapmalıdır.
4.6. İstemci yazılımı girilen komutlara göre biyometrik doğrulama ve biyometrik kayıt işlemlerini gerçekleştirecek, işlem adımlarını operatörün, üzerindeki ekrandan takip etmesini sağlayacak, biyometrik görüntünün alınması sırasında görüntülü yönlendirme yapacak şekilde tasarlanmalıdır.
4.7. İstemci yazılımı, sunucu yazılımı ile Secure Socket Layer üzerinden ve en az 128 bit anahtar uzunluğu kullanılarak iletişime geçecektir.
4.8. İstemci yazılımı, güvenlik sebebi ile; biyometrik bilgileri, biyometrik sensörün 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 şifrelemelidir.
4.9. İstemci yazılımı, güvenlik sebebi ile okuyucu sensör ile istemci cihazı arasındaki biyometrik veri 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 şifreleyip ve iletilebilmelidir.
4.10. Okuyucu sensör, okuma işleminin hemen ardından, biyometrik veri istemci cihaza gönderilmeden biyometrik bilgileri geri dönüşümsüz bir algoritmadan geçirecek, orijinal biyometrik görüntüyü tutmayacak ve daha sonra istemci cihazına biyometrik bilgi iletilecektir. Algoritmadan geçirilen veriden orijinal biyometrik imaja dönülmesi mümkün olmayacaktır.

4.11. İstemci yazılımı, belirlenecek özel durumların merkeze bildirilebilmesine imkan sağlayacak altyapıda olacaktır. (Örneğin hastanın uygun eli veya parmağının olmaması gibi.
4.12. İstemci yazılımı, hastalara ait TC Kimlik numaralarının hatalı girilmesini engelleyecek yazılımsal kontrollere sahip olmalıdır. İstemci yazılımı, ilk kurulum işlemi sırasında ve hastane, poliklinik bilgilerinin değiştirilmesi durumunda merkez ile iletişime geçip, aktivasyon işlemi yapılmadan kayıt doğrulama işlemi yapılmasına imkan vermeyecektir.
4.13. İstemci yazılımı, üzerinde oluşabilecek problemlere karşı, üzerinde tuttuğu hata ve sistem loglarını merkeze gönderebilecek özelliğe sahip olmalıdır.
4.14. İstemci sistemi ve yazılımı üzerinde kesinlikle kalıcı olarak biyometrik veri bulundurulmayacak ve işlenmeyecektir
4.15. İstemci yazılımı ve istemcinin çalışması için herhangi bir başka bilgisayar ve yazılıma gerek duyulmayacak, sistem kendi başına stand-alone çalışacak yapıda olmalıdır.
4.16. Veri merkezi ve sağlık sunucularında konumlandırılan(Uçtan uca) tüm cihazların güvenliği Tübitak tarafından incelenecek olup herhangi bir güvenlik eksiği olması durumunda Yüklenici tüm ürünleri için hiçbir hak iddia etmeden cihazlar ve yazılımlar üzerinde gerekli değişiklikleri yapacaktır
4.17. BKDÜ cihazlarının teknik özellikleri kurumun mevcut altyapısında bulunan diğer biyometrik teknolojilerinden daha düşük özellikte olmayacaktır.
4.18. Veri merkezinde konumlandırılan cihazların sistemin çalışması noktasındaki performansı kurumun mevcut altyapısında bulunan diğer biyometrik teknolojilerin performansından düşük olamaz. Sistemin performansının eksik olduğu düşünüldüğü durumda veri merkezine yeni ürünler eklenecektir.

EK 1-(2-D)

2.TİP BİYOMETRİK KİMLİK DOĞRULAMA SİSTEMİ SEÇENEĞİ

(2-D)- Parmak Damar İzi Sistemi Biyometrik Kimlik Doğrulama Ünitesinin Bileşenleri

1. Biyometrik Kimlik Doğrulama Ünitesi (BKDÜ)

1.1. BKDÜ Donanımı Bakım ve Kurulumu

1.1.1. Cihaz ile birlikte çalışması için gerekli tüm çevre-birimler/donanım teslim edilecektir.
1.1.2. Altyapı ve kablolama ürünü satın alan SHS'ler tarafından hazırlanmış olacaktır.
1.1.3. Cihaz devreye alınması sırasında gerekli olacak tüm bilgiler SHS tarafından belirlenmiş olan kurulum sorumlusuna iletilecektir.
1.1.4. Cihaz arızaları için donanım değişimi yapılarak çözüm sağlanacaktır.
1.1.5. Cihazın; yazılım güncellemelerini merkezi, otomatik ve SSL güvenliği ile yapılabilmesi sağlanmalıdır.
1.1.6. Cihazların merkezi sistem ile takip edilebilmesi sağlanmalıdır.
1.1.7. Cihazda oluşacak sorunlar için kolay, anlaşılır ve görüntülenebilir hata kodları üretilmesi sağlanmalıdır.
1.1.8. Cihaz sorunları için uzaktan destek verilmesine olanak sağlanmalıdır.
1.1.9. Cihaz ilk kurulum/devreye alınma hizmeti standart olarak verilmelidir.
1.1.10. Cihazın fiziksel sorunlarından dolayı değişimi en fazla 5 iş gününde sağlanmalıdır.
1.1.11. Cihaz 2 yıl standart garanti ile satışı yapılacak olup, 10 yıl yedek parça sağlanmalıdır.
1.1.12. Cihazlar, sevk esnasında sigortalı olarak taşınmalıdır.
1.1.13. Cihazlar SHS'lerdeki ilk kurulum ve sonraki tüm servis işlemleri için sadece yetkili servis elemanlarının biyometrik verisi ile müdahaleye müsaade edecek yapıya sahip olmalıdırlar.

1.2. Biyometrik Kimlik Doğrulama Terminali

1.2.1. BKDÜ; 7 gün 24 saat esasına göre ve 5°C ila 45°C sıcaklık aralığında kesintisiz olarak çalışabilecektir.
1.2.2. BKDÜ üzerinde fan bulunmayacaktır.
1.2.3. BKDÜ; harici olarak farklı cihazlar ile boot edilemeyecektir.
1.2.4. BKDÜ'ne harici olarak biyometrik verileri depolamak amacı ile başka bir aygıt bağlanmayacaktır.
1.2.5. BKDÜ, kişinin TC Kimlik No ve Biyometrik Kimlik bilgilerini kriptolayarak ana sunucuya transfer edecek teknolojiye sahip olacaktır.
1.2.6. BKDÜ sadece tek bir Parmak Damar izi Sensörü bağlantısına izin verecektir.
1.2.7. BKDÜ, TÜBİTAK'ın geliştirdiği ve 2013 yılında Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün devreye almayı planladığı yeni Kimlik Kartının ve üzerindeki canlı doku desteği olan biyometrik şablonlardan en az bir tanesini destekleyebilmelidir.
1.2.8. BKDÜ de en az 1 adet 10/100Mbit lik ethernet adaptörü olacaktır.
1.2.9. BKDÜ; şebekedeki voltaj dalgalanmalarına karşı, ürünün stabilitesini ve devamlılığını sağlamak adına voltaj koruma sistemine sahip olacaktır.
1.2.10. BKDÜ; yetkisiz kişilerce, fiziksel olarak açılmaya karşı korumalı olacaktır. Sistem, yetkisiz kişilerce açılsa dahi kendini bloke edecek ve çalışmasını durduracak şek ilde tasarlanmış olacaktır.
1.2.11. Cihazi; İnsan sağlığını tehlikeye sokacak herhangi bir ürün grubunda olmamalıdır ve herhangi bir zararlı madde içermemelidir.
1.2.12. Cihaz; Elektromanyetik Uyumluluk Yönetmeliği (1999/519/EC, 2004/108/EC ve 2006/95/EC) ile uyumlu olup aşağıdaki standartlara uygun olacaktır.
1.2.13. EN 50364 (2001)
1.2.14. EN 50357 (2001)
1.2.15. EN 55022 (2006 +A1/2007)
1.2.16. EN 55024 (1998 + A1/2001 + A2/2003
1.2.17. EN 60950-1:2006 + A11/2009
1.2.18. ES 203021-1/2/3
1.2.19. TR103000-1/2/3/4
1.2.20. Cihaz CE sertifikasına sahip olacaktır.

1.2.21. BKDÜ, tekil ve değiştirilemez bir tanımlayıcıya sahip olacaktır. Bu sayede merkezi olarak onay verilmemiş sistemlerin kullanımı engellenebilecek ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilecektir.
1.2.22. BKDÜ üzerinde kullanıcının TC Kimlik bilgisini girmesine olanak tanıyacak 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, Sil, İptal, Giriş tuşlarının yer aldığı PCI PED 2.0 onaylı tuş takımı ve F1, F2, F3, F4 programlanabilir fonksiyon tuşlarını içeren tuşlar bulunacaktır. Cihaz ayrıca bir klavyeye ihtiyaç duymayacaktır.
1.2.23. Cihaz EMV Level 1 ve EMV Level 2 sertifikasına sahip olmalıdır.
1.2.24. Cihaz APAC Common Criteria sertifikasına sahip olmalıdır.
1.2.25. Cihaz, CE ve RoHS sertifikasına sahip olacaktır.
1.3. Parmak Damar izi Sensörü
1.3.1. Parmak Damar izi tarama metodu; daha yüksek hassasiyet ve güvenliğe ulaşabilmek için, tüm parmak biyometrisini okumalı, tümleşik (multimodal) bir parmak biyometrisi verisi oluşturmalıdır. Parmak Damar izi sensörü damar haritasını okuma ve aktarmadan önce kendi üzerinde RSA 2048 bit algoritma ve anahtar uzunluğu ile şifreleme özelliğine sahip olacaktır.
1.3.2. Parmak Damar izi sensöründen veri çıkışı (Biyometrik Kimlik Doğrulama Ünitesine) tamamen güvenli ve kriptolu olmalıdır. Bu verinin tüm arabirimler arası iletiminde veri şifreli olarak taşınmalıdır. Verinin üretilmesi ile doğrulanmasına kadar her aşama (uçtan uca) güvenli olmalıdır. Bu amaçla 256Bit SSL güvenliği oluşturabilmelidir.
1.3.3. Parmak Damar izi sensörü FIPS 201 ve MINEX uyumluluğuna sahip olmalıdır.
1.3.4. Parmak Damar izi sensörü FBI PIV IQS sertifikasına sahip olmalıdır.
1.3.5. Parmak Damar izi sensörü, çevrim içi olarak (online) 1:1 kimlik doğrulamayı kendi üzerinde yapabilmelidir. Parmak Damar izi sensörü üzerinde okunan biyometrik veri ile ilgili hiç bir kayıt yapılmayacak, okunan verileri kayıt edilmesi engellenmiş olacaktır.
1.3.6. Parmak Damar izi sensörü, üzerindeki özel algoritma yazılımı ile erişkin ve çocukları ayırabilmeli, gerektiğinde otomatik olarak çocuk algoritmasını çalıştırabilmelidir.
1.3.7. Parmak Damar izi sensörünün FAR değeri % 0.000001 ve FRR değeri % 0,001 den büyük olmayacaktır.
1.3.8. Parmak Damar izi sensörü, FAR ve FRR değerlerini tek bir biyometrik okuyucu ile sağlamalıdır.
1.3.9. Parmak Damar izi sensörü, insan sağlığına zararlı ürün sınıfında olmamalıdır. Gerekli EyeSafe sertifikalarına sahip olmalıdır.
1.3.10. Parmak Damar izi sensörü, canlı doku tespit (Life Detection) özelliğine sahip olmalıdır.
1.3.11. Parmak Damar izi sensörünün çalışma sıcaklığı en az -10 °C ile 50 °C aralığında olmalıdır. Parmak Damar izi sensörü, tekil ve değiştirilemez bir tanımlayıcıya sahip olmalıdır. Bu sayede merkezi olarak onay verilmemiş sensörlerin kullanımı engellenebilmeli ve tüm uç noktadaki cihazlar merkezi olarak kontrol edilebilmelidir. Bu amaçla üzerinde sertifika barındırabilmelidir.
1.3.12. Parmak Damar izi Sensörü CE, FCC standartlarına sahip olmalıdır.
1.3.13. Parmak Damar izi Sensörü RoHS, REACh ve WEEE çevre standartlarına sahip olmalıdır.
1.4. BKDÜ Yazılımı
1.4.1. BKDÜ yazılımı, Sistemin internete çıkabilmesi için gerekli bilgilerin girilmesine imkân sağlayacaktır. IP, SubnetMask, Gateway, DNS Server ayarları cihazda güvenli ortamda ayarlanmış olarak saklanmaktadır. Güvenlik nedeni ile kullanıcının bu ayarlara erişimine izin verilmemektedir.
1.4.2. BKDÜ yazılımı, SHS'larının ID numarasının, Poliklinik ID'lerinin ve Onaylı SHS personelinin ID'lerinin girilmesine imkan sağlayacaktır.
1.4.3. BKDÜ yazılımı, sistemin network ve internete erişebilirliğinin tespit edilmesi için kullanımı kolay network tanımlama araçlarına sahip olacaktır.
1.4.4. BKDÜ yazılımı, merkezi sistem üzerinden istenildiği zaman güvenli şekilde güncellenebilmelidir.
1.4.5. BKDÜ yazılımı, üzerinde çalışan işletim sistemi ile ilgili güncellemeler merkez tarafından yayınlandığı takdirde, merkezden gerekli verileri güvenli ortamda kendi üzerine çekebilmeli, yazılım güncellemelerini kullanıcı müdahalesine gerek kalmadan yapmalıdır.

1.4.6. BKDÜ yazılımı girilen komutlara göre biyometrik doğrulama ve biyometrik kayıt işlemlerini gerçekleştirecek, işlem adımlarını operatörün, üzerindeki ekrandan takip etmesini sağlayacak, biyometrik görüntünün alınması sırasında yazılı ve görüntülü yönlendirme yapacak şekilde tasarlanmalıdır.
1.4.7. BKDÜ yazılımı, sunucu yazılımı ile Secure Socket Layer üzerinden ve en az 128 bit anahtar uzunluğu kullanılarak iletişime geçecektir.
1.4.8. BKDÜ yazılımı, güvenlik sebebi ile biyometrik sensörün içerisinde oluşturduğu biyometrik şablonu, biyometrik sensörün içerisinde AES, DES, Triple DES gibi dünyada kabul görmüş simetrik şifreleme algoritmaları ile ve en az 256 bit şifre anahtar uzunluğu kullanılarak şifrelemeli ve/veya RSA 1024/2048 bit anahtar ile asimetrik olarak imzalamalıdır.
1.4.9. BKDÜ yazılımı, güvenlik sebebi ile sensör ile BKDÜ arasındaki biyometrik veri içerisinde AES, DES, Triple DES gibi dünyada kabul görmüş simetrik şifreleme algoritmaları ile ve en az 256 bit şifre anahtar uzunluğu kullanılarak şifreleyip ve iletilebilmelidir.
1.4.10. Sensör, okuma işleminin hemen ardından, biyometrik veri BKDÜ'ye gönderilmeden biyometrik bilgileri geri dönüşümsüz bir algoritmadan geçirecek, orijinal biyometrik görüntüyü tutmayacak ve daha sonra BKDÜ'ye biyometrik şablon iletilecektir. Algoritmadan geçirilen veriden orijinal biyometrik imaja dönülmesi mümkün olmayacaktır.
1.4.11. BKDÜ yazılımı, belirlenecek özel durumların merkeze bildirilebilmesine imkan sağlayacak altyapıda olacaktır. (Örneğin hastanın uygun eli veya parmağının olmaması gibi.)
1.4.12. BKDÜ yazılımı, hastalara ait TC Kimlik numaralarının hatalı girilmesini engelleyecek yazılımsal kontrollere sahip olmalıdır. İstemci yazılımı, ilk kurulum işlemi sırasında ve hastane, poliklinik bilgilerinin değiştirilmesi durumunda merkez ile iletişime geçip, aktivasyon işlemi yapılmadan kayıt doğrulama işlemi yapılmasına imkan vermeyecektir.
1.4.13. BKDÜ yazılımı, üzerinde oluşabilecek problemlere karşı, üzerinde tuttuğu hata ve sistem loglarını merkeze gönderebilecek özelliğe sahip olmalıdır.
1.4.14. BKDÜ ve yazılımı üzerinde kesinlikle kalıcı olarak biyometrik veri bulundurulmayacak ve işlenmeyecektir.
1.4.15. BKDÜ yazılımı ve BKDÜ'nün çalışması için herhangi bir başka bilgisayar ve yazılıma gerek duyulmayacak, sistem kendi başına stand-alone çalışacak yapıda olmalıdır.
1.4.16. Veri merkezi ve sağlık sunucularında konumlandırılan (Uçtan uca) tüm BKDÜ cihazların güvenliği Tübitak tarafından incelenecek olup herhangi bir güvenlik eksiği olması durumunda Yüklenici tüm ürünleri için hiçbir hak iddia etmeden BKDÜ cihazları ve yazılımları üzerinde gerekli değişiklikleri yapacaktır.
1.4.17. BKDÜ cihazlarının teknik özellikleri kurumun mevcut altyapısında bulunan diğer biyometrik teknolojilerinden daha düşük özellikte olmayacaktır.
1.4.18. Veri merkezinde konumlandırılan cihazların, sistemin çalışması noktasındaki performansı kurumun mevcut altyapısında bulunan diğer biyometrik teknolojilerin "kayıt alma ve doğrulama" performansından düşük olamaz. Sistemin "kayıt alma ve doğrulama" performansının eksik olduğu düşünüldüğü durumda veri merkezine yeni ürünler eklenecektir.

EK:2

EK 2. Rıza Formu

RIZA FORMU

Sağlık hizmetlerinden faydalanabilmek için 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 67 inci maddesine göre kimlik doğrulaması yapılabilmesi amacıyla biyometrik verilerinin alınmasına muvafakat ediyorum.

Tarih
TC Kimlik No
İsim Soyisim

İmza