



DOĐUŐ ÜNİVERSİTESİ

TURNİKE & PDKS SİSTEMİ TEKNİK ŐARTNAMESİ

TEKNİK ŐARTNAMESİ

1. AMAÇ

Bu teknik şartname; Doğuş Üniversitesi bünyesinde hâlihazırda kullanılan Meyer turnike sisteminin tamamen yenilenmesini, yüz tanıma – kart – QR destekli yeni nesil turnike cihazlarının devreye alınmasını, öğrenci ve personel bilgilerinin Proliz ve SAP sistemleri üzerinden otomatik olarak yönetilmesini, kullanıcı durum kontrollerinin sağlanmasını ve tüm geçiş hareketlerinin raporlanabileceği modern bir PDKS (Personel Devam Kontrol Sistemi) altyapısının kurulmasını amaçlamaktadır.

Bu kapsamda sistem; akademik, idari personel, öğrenciler ve misafir kullanıcıların kurumsal güvenlik standartlarına uygun şekilde kontrollü geçişini sağlayacak biçimde tasarlanacaktır.

2. KAPSAM

Bu teknik şartname aşağıdaki unsurları kapsamaktadır:

- Mevcutta kullanılan tüm Meyer turnike cihazlarının değiştirilmesi
- Yüz tanıma + Kart + QR destekli yeni turnike sistemlerinin kurulumu
- Proliz – SAP – Mobil Uygulama entegrasyonlarının sağlanması
- Kullanıcıların (öğrenci / personel) otomatik oluşturulması ve durum kontrolü
- Yasaklı / engelli kullanıcıların sistem tarafından engellenmesi
- Tüm geçiş kayıtlarının merkezi panelden izlenmesi
- Raporlama altyapısının kurulumu
- Sistem için gerekli tüm donanım, yazılım ve entegrasyon çalışmalarının yapılması
- Mobil uygulama ile QR üretimi ve geçmiş görüntüleme fonksiyonları

Sistem; **Faz 1 (Personel)** ve **Faz 2 (Öğrenci yüz tanıma)** şeklinde iki aşamalı olarak devreye alınacaktır.

3. GENEL TEKNİK ÖZELLİKLER

3.1 Faz Yapısı

Faz 1 – Personel Geçiş Sistemi

- Tüm Meyer cihazları sökülerek yeni nesil cihazlar takılacaktır.
- Yüz tanıma yalnızca akademik ve idari personelde aktif olacaktır.
- Öğrenciler bu fazda **kart + QR** ile giriş yapacaktır.

Faz 2 – Öğrenci Yüz Tanıma Aktivasyonu

- Yüz tanıma sistemi öğrencilere de açılacaktır.
- KVKK kapsamında gerekli izin/onay ekranları bu fazda devreye alınacaktır.

4. DONANIM GEREKSİNİMLERİ

4.1 Turnike Cihazı Özellikleri

a. Yüz Tanıma

- Tanıma süresi: ≤ 0.3 saniye
- Maskeli yüz tanıma desteği
- Minimum doğruluk oranı: %99
- Düşük ışık / ters ışıkta çalışabilme
- Biyometrik verilerin KVKK uygun şifreleme ile saklanması

b. Kart Okuyucu

- Mevcut kurum kart standardı ile tam uyumluluk (Mifare/Proximity vb.)
- Personel / öğrenci / misafir kart ayrımı

c. QR Kod Okuyucu

- Mobil uygulama üzerinden dinamik, tek kullanımlık, zaman kısıtlı QR kodları okuyabilme

d. Anti-Passback

- Aynı kişinin arka arkaya geçiş yapmasını engelleme mekanizması bulunmalıdır.

e. Donanım Özellikleri

- IP65 koruma sınıfı
- 2 GB RAM – 16 GB ROM (minimum)
- TCP/IP, WiFi, RS485 destekleri
- Offline çalışabilirlik (internet yokken lokal log oluşmalı)

5. YAZILIM VE SİSTEM ALTYAPISI

5.1 Kullanıcı Yönetimi ve Entegrasyonlar

a. Proliz Entegrasyonu

- Öğrenci kaydı olduğunda turnike sistemi kullanıcıyı otomatik oluşturmalıdır.
- Öğrenci durumu (aktif/pasif/mezun) anlık olarak kontrol edilmelidir.
- Yasaklı öğrencilerin geçişi otomatik engellenmelidir.

b. SAP Entegrasyonu

- Personel işe giriş/çıkış durumları SAP HR ile uyumlu olmalıdır.
- Yeni personel oluşturulduğunda cihazlara otomatik aktarım olmalıdır.
- İşten ayrılan personel otomatik engellenmelidir.

c. Yasaklı / Engelli Kullanıcı Kontrolü

- Panele veya cihazlara kullanıcı durum bilgisi anlık yansıtılmalıdır.
- Ekranda: "GEÇİŞ İZİNİ YOK – HESAP PASİF" gibi uyarılar gösterilmelidir.

d. Biyometrik Veri Yönetimi

- Yüz tanıma şablonları AES-256 gibi güçlü bir algoritma ile şifreli tutulmalıdır.
- KVKK uyumluluğu zorunludur.

6. GEÇİŞ SENARYOLARI

6.1 Personel

- Yüz Tanıma
- Kart
- QR (yedek yöntem)

6.2 Öğrenci

- Faz 1: **Kart + QR**
- Faz 2: **Yüz + Kart + QR**

6.3 Misafir

- Geçici kart
- Mobil uygulama veya güvenlik birimi üzerinden oluşturulan QR kod

7. MOBİL UYGULAMA ENTEGRASYONU

- Tek kullanımlık, zaman kısıtlı QR kod üretimi
- Turnike geçişlerinde anlık bildirim
- Kullanıcının kendi giriş-çıkış geçmişini görüntülemesi
- (Opsiyonel) yüz verisinin mobil uygulamadan yüklenebilmesi

8. YÖNETİM PANELİ (BACKOFFICE)

8.1 Kullanıcı Yönetimi

- Öğrenci ve personelin otomatik oluşturulması
- Yasaklı/engelli kullanıcıların takibi
- Manuel kullanıcı ekleme/düzenleme

8.2 Cihaz Yönetimi

- Online/offline durum takibi
- Log miktarı ve trafik yoğunluğu görüntüleme

8.3 Turnike Yönetimi

- Giriş-çıkış kayıtları
- Anti-passback logları
- Filtrelenebilir hareket geçmişi

8.4 Entegrasyon Yönetimi

- SAP – Proliz – Mobil uygulama bağlantı durumu
- Hata/uyarı izleme

9. RAPORLAMA ALT YAPISI

9.1 Personel Raporları

- Giriş-çıkış saatleri
- Mesai uyum raporları
- Devam-devamsızlık analizleri

9.2 Öğrenci Raporları

- Giriş yoğunluk raporları
- Yasaklı kullanıcı giriş denemeleri

9.3 Sistem Raporları

- Cihaz online/offline raporu
- Sistem performans raporları
- Entegrasyon hata raporları

9.4 Çıktı Formatları

- Excel
- PDF
- CSV

10. GÜVENLİK GEREKSİNİMLERİ

- Tüm iletişim TLS 1.2 ve üzeri ile şifrelenmelidir.
- Kart, QR ve yüz tanıma verileri şifreli olarak saklanmalıdır.
- Parmak izi teknolojisi **kullanılmayacaktır**.
- Yetkisiz erişim loglanmalıdır.

11. PERFORMANS GEREKSİNİMLERİ

- Yüz tanıma süresi: **0.3 – 0.5 saniye**
- Cihaz açılış süresi: **≤ 10 saniye**
- Geçiş doğrulama süresi: **≤ 1 saniye**
- Senkronizasyon gecikmesi: **≤ 30 saniye**

12. TEST VE KABUL SÜRECİ

12.1 Fonksiyonel Testler

- Yüz tanıma, kart, QR geçişleri
- Anti-passback
- Offline geçiş senaryoları

12.2 Entegrasyon Testleri

- Proliz
- SAP
- Mobil uygulama
- Yönetim paneli

12.3 Performans Testleri

- Eş zamanlı geçiş dayanımı
- Gecikme testleri

12.4 Güvenlik Testleri

- KVKK uyumluluğu
- Kimlik doğrulama güvenliği
- Log güvenliği

12.5 Kullanılabilirlik Testleri

- Cihaz ekranı
- Yönetim paneli arayüz deneyimi

13. EĞİTİM VE DESTEK

- Akademik ve idari personel için kullanıcı eğitimi
- Güvenlik personeline turnike kullanım eğitimi
- Yönetim paneli teknik eğitimi
- Destek – bakım süreçleri sözleşmede belirtilmelidir
- SLA süreleri açıkça tanımlanmalıdır