

## **Mobiliz Filo Yönetim Sistemlerinde İnternet Protokol Güvenliđi**

Mobiliz Bilgi ve İletişim Sistemleri A.Ş. tarafından sağlanan Mobiliz uygulamalarında sistemin iletişim akışı aşağıdaki gibidir:

1. Mobil birimlerle merkez sunucu arasındaki iletişim,
2. Sistem kullanıcıları ile merkez sunucu arasındaki iletişim.

### **1.1. Mobil birimlerle merkez sunucu arasındaki iletişim:**

Mobil birimler ile olan erişim:

1. GSM/GPRS şebekesi üzerinde GPRS mesajlaşması yoluyla APN erişimi, GSM şebekesindeki sayısal sistem ve kodlama güvenliđi ile korunur.
2. Her paket içinde giden sayısal veriler sadece üreticinin bildiđi özel formattadır.
3. Mobil birimler belli aralıklarla deđişen dinamik IP ile sisteme kaydedildikleri için birimlerin IP adresine göre takibi mümkün deđildir.
4. APN ile merkez sunucu arasındaki internet bağlantısı, VPN üzerinden sağlanarak şifrelenir ve yabancıların bu mesajlaşmaya müdahalesi önlenir.
5. Özetle, sisteme araçların bağlandıkları tek IP portu VPN üzerinden güvenli bir bağlantı ile yapılmaktadır.

### **1.2. Sistem kullanıcıları ile merkez sunucu arasındaki iletişim:**

Uygulamanın internete açılması, kullanıcının seçimine bađlıdır. İstenirse sistem erişimi sadece intranet içinde tutulabilir. Şayet herhangi bir internet bağlantısından sistemdeki WEB sunucusuna erişebilmek istenirse aşağıdaki yöntemler uygulanır.

WEB kullanıcılarının gezginci kullanarak sisteme erişimleri:

1. Kullanıcıların sisteme erişimleri kullanıcı adı ve şifre yöntemi ile yapılmaktadır.
2. Sisteme giriş şifreleri veritabanında MD5 hash algoritmasından geçirilerek kaydedilmektedir. Bu sayede herhangi bir şekilde (bakım amaçlı vb) veritabanına erişilse bile orada kayıtlı kullanıcılara ait şifrelerin açık haline erişilememektedir.
3. WEB arabağlantısında SSL kullanılabilenkte, kullanıcı bilgileri ve diđer bilgiler şifrelenebilmektedir.
4. Erişimin belli IP adresleri dışından yapılması engellenebilir.
5. Veri tabanına kullanıcıların doğrudan erişimi yoktur. Sadece sunucu üzerinden erişilebilir.
6. Özetle sadece http ve https ulaşım portu açılarak kullanıcıların sisteme SSL kullanan güvenli bir bağlantıyla girmeleri sağlanır.

### **1.3. Firewall Kullanımı:**

Yukarıdaki bahsi geçen 3 port dışındaki portlar firewall ile korunarak sistem güvenliđi sağlanabilir.

### **1.4. Ek Güvenlik:**

Özel durumlar için birimin (lokasyon vb) bilgi göndermesini önleyen bir anahtar sisteme eklenebilir (privacy mode).