TRtest
Test ve Değerlendirme A.Ş.

GÜVENLİ MESAJLAŞMA ÜRÜN GRUBU TEST KRİTERLERİ

No	Başlık/Soru	C (Giriş Seviye)	B (Orta Seviye)	A (Üst Seviye)
UG	**1- Ürün Güvenliği**			
UG_YA	**Yönetim Arayüzleri**			
UG_YA_AZT	**Arayüz Zayıflık Taraması**			
UG_YA_AZT_1	Zararlı girdi (Input Validation) kontrolü yapılıyor mu?	C		
UG_YA_AZT_2	Kimlik Doğrulama kontrolü yapılıyor mu?	C		
UG_YA_AZT_3	İki faktörlü doğrulama yapılıyor mu?	C		
UG_YA_AZT_4	Erişim yönetimi ve yetkilendirme yapılıyor mu?	C		
UG_YA_AZT_5	Hata yönetimi ve loglama işlemleri en az aşağıdakileri sağlıyor mu? • İşlemi yapan kullanıcı (gerçek kişi veya yazılımsal süreç için tanımlanmış kullanıcı) bilgisi • İşlem zamanı • Kaynak ve hedef sistem tanımlayıcı bilgileri (ip, sunucu adı vb.) • İşlem özeti (başarılı işlem, başarısız işlem vb..)	C		
UG_YA_AZT_6	Loglar chain yapısı bulunduruyor mu?			A
UG_YA_AZT_7	Loglar periyodik olarak imzalanıyor mu?		B	
UG_YA_AZT_8	Bilinen zafiyeti olmayan güvenli iletişim kanalları destekleniyor mu?	C		
UG_YA_AZT_9	Veri tabanında hassas verilerin güvenliği sağlanıyor mu?	C		
UG_YA_AZT_10	Oturum yönetiminde yetki kontrolü yapılıyor mu?	C		
UG_YA_AZT_11	Parola yönetimi güvenliği (parola karmaşıklığı) sağlanıyor mu?	C		
UG_YA_AZT_12	Kullanıcının kişisel veri gizliliği (KVKK Uyumluluk) sağlanıyor mu?	C		
UG_YA_AZT_13	Çıktı Kodlama (Output encoding) yapılıyor mu?	C		
UG_MUZT	**Mobil Uygulama Zayıflık Taraması**			
UG_MUZT_1	Zararlı girdi kontrolü yapılıyor mu?	C		
UG_MUZT_2	Kimlik Doğrulama aşamasında kaba kuvvet kontrolü yapılıyor mu?	C		
UG_MUZT_3	Erişim yönetimi ve yetki kontrolü yapılıyor mu?	C		
UG_MUZT_4	Hata yönetimi ve loglama işlemleri yapılıyor mu?	C		
UG_MUZT_5	Bilinen zafiyeti olmayan güvenli iletişim kanalları destekleniyor mu?	C		
UG_MUZT_6	Kullanıcının kişisel veri gizliliği (KVKK Uyumluluk) sağlanıyor mu?	C		

UG_MUZT_7	İstemci tarafında tüm güvenlik kontrolleri sunucu tarafında da yapılıyor mu?	C		
UG_MUZT_8	Gerektiğinde kullanıcıları güncelleme yüklemeye zorlayan kontroller var mı?	C		
UG_MUZT_9	Şifreleme anahtarı ve parola gibi hassas değerler işletim sisteminin güvenli depolama alanlarında mı tutuluyor?	C		
UG_MUZT_10	Uygulama verilerinin dahili hafıza dışında (SD Card vb.) tutulmaması sağlanıyor mu?			A
UG_MUZT_11	Uygulamanın 3. parti sistemlere hassas veri transferi (ad, soyad, telefon numarası, mesaj içeriği, e-posta, şirket bilgisi, çağrı kayıtları, özel nitelikli kişisel veriler) yapmadığı teyit ediliyor mu?	C		
UG_MUZT_12	Klavye önbelleği uygulama içinde kapatılabiliyor mu?		B	
UG_MUZT_13	IPC (Uygulamalar arası iletişim) mekanizması ile 3. parti uygulamalara veri aktarmadığı teyit ediliyor mu?	C		
UG_MUZT_14	Kullanıcı arayüzünde parola, pin, şifreleme anahtarı gibi değerler perdeleniyor mu?	C		
UG_MUZT_15	Uygulamanın aldığı yedekler varsayılan olarak şifreleniyor mu?		B	
UG_MUZT_16	Uygulama arka plana atıldığında son kullanılan uygulamalar listesinde ekran görüntüsünü gizleyebiliyor mu?		B	
UG_MUZT_17	Uygulama belleğinde, hassas veri kullanımı bittikten sonra siliniyor mu?			A
UG_MUZT_18	Uygulama kodunda şifreleme anahtarının gömülü olmadığı teyit ediliyor mu?	C		
UG_MUZT_19	Kriptografi uygulamalarında zayıflığı bilinen algoritma kullanılmadığı teyit edildi mi?	C		
UG_MUZT_20	Uygulama şifreleme işlemleri için güvenli rastgele numara üreticilerini kullanıyor mu?	C		
UG_MUZT_21	Uygulama uçtan uca şifreleme yapıyor mu?	C		
UG_MUZT_22	Hassas işlemler için step-up authentication kullanılıyor mu? (işlem bazında ekstra güvenlik adımı)			A
UG_MUZT_23	Kullanıcılar sisteme giriş yaptıkları cihazların listesini görebiliyor mu?	C		
UG_MUZT_24	Uygulama SSL pinning yapıyor mu?	C		
UG_MUZT_25	Uygulamanın ihtiyaç duymadığı izinleri almadığı teyit edildi mi?	C		
UG_MUZT_26	WebView kullanılıyorsa, view içine şifresiz trafik yüklenmediği teyit ediliyor mu?	C		
UG_MUZT_27	WebViewlar üzerinde kullanılmayan özelliklerin kapatılması için sıkılaştırma yapılmış mı?	C		
UG_MUZT_28	Hassas işlemler yapan Native metodların Webview içinden çağırılmadığı teyit ediliyor mu?	C		
UG_MUZT_29	Uygulamayı imzalamak için kullanılan anahtar güvenli bir şekilde saklanıyor mu?	C		
UG_MUZT_30	Uygulama debug özellikleri kapatılarak mı derlenmiş?	C		
UG_MUZT_31	Uygulama içinde kullanılan 3. parti kütüphaneler güvenlik testlerinden geçirilmiş mi?			A
UG_MUZT_32	Uygulama jailbreak ve root yapılmış sistemleri tanıyabiliyor mu?	C		
UG_MUZT_33	Uygulama jailbreak ve root yapılmış sistemlerde çalışmayı reddedebilme seçeneği var mı?		B	
UG_MUZT_34	Uygulama debugger bağlanmasına karşı bir önlem almış mı?			A

UG_MUZT_35	Uygulama yeniden paketlemeye karşı bir önlem almış mı?	C		
UG_MUZT_36	Uygulama emülatör içinde çalışıp çalışmadığını kontrol ediyor mu?	C		
UG_MUZT_37	Uygulama emülatör içinde çalışmayı reddebiliyor mu?		B	
UG_MUZT_38	Uygulama koduna perdeleme yapılmış mı?	C		
UG_MUZT_39	Tüm kaynaklara (API anahtarları, sertifikalar, kütüphaneler vb.) perdeleme yapılmış mı?		B	
UG_MUZT_40	Export edilen tüm bileşenler(activity, provider, receiver, service) bir izin ile korunuyor mu?(android)	C		
UG_MUZT_41	Uygulama tarafından tanımlanan izinler uygun güvenlik seviyeleri ile tanımlanmış mı?	C		
UG_MUZT_42	Uygulama ekranlarında overlay saldırılarına karşı önlem alınmış mı? (android)	C		
UG_MUZT_43	Uygulama tavsiye edilen en yüksek API seviyesi için derlenmiş mi? (Android)	C		
UG_MUZT_44	Statik kod analizi yapılmış mı?	C		
UG_MUZT_45	Uygulama kendi içinde bir ekran kilidi mekanizmasına sahip mi?	C		
UG_MUZT_46	Uygulama karşı tarafın parmak izini (fingerprint – security code) doğrulayabiliyor mu?			A
UG_MUZT_47	Kontak yükleme, işleme, günlük mesaj atma, anlık ses görüşmesi limiti vb. konularda kullanıcı aktivitelerine sınır getirilebiliyor mu?		B	
GFT	**2- Güvenlik Fonksiyon Testi**			
GFT_YT	**Yetkilendirme Testleri**			
GFT_YT_1	Yetkilendirme (authorization) mekanizması kapsamında kullanıcı ve rol bazlı yetkilendirme yapabiliyor mu?		B	
GFT_YT_2	Push Notification kanalları üzerinde kullanıcının kişisel verileri taşınmadığı teyit ediliyor mu?	C		
GFT_YT_3	İstemci/Sunucu arası tüm iletişim güvenli protokoller üzerinden yapılıyor mu?	C		
GFT_YT_4	Cihaz tipine göre sunucu tarafında ayrı oturum yönetimi yapılıyor mu?	C		
GFT_YT_5	Belirlenen kullanıcıların kullanımı engellenebiliyor mu ?	C		
GFT_YT_6	Farklı cihazlardan oturum açıldığında açık oturuma/oturumlara bilgilendirme mesajı gidiyor mu?	C		
GFT_YT_7	Sunucu loglarda kullanıcının değerli bilgileri maskelenmiş bir şekilde yazılıyor mu?	C		
GFT_YT_8	Çok fazla izinsiz giriş denemesinde hesap askıya alınıyor mu?	C		
GFT_YT_9	Alıcıya iletilen mesajlar sunucudan silinebiliyor mu? (Böyle bir opsiyon sunulabiliyor mu?)	C		
GFT_YT_10	Sunucuda tutulması gereken veriler şifrelenmiş olarak saklanıyor mu?	C		
GFT_YT_11	Telefonda tutulan veriler (mesaj, medya) şifreli olarak tutuluyor mu?			A
GFT_YT_12	Uygulamada kullanılan kriptografik anahtarların üretilmesi, kullanımı, saklanması donanım destekli (Akıllı Kart, TEE, Secure Enclave vb.) güvenilir ortamda yapılıyor mu?			A
TO	**3- Temel Özellikler**			

TO_1	Kimlik doğrulama ve yetkilendirme destekleniyor mu?	C		
TO_2	Sesli ve görüntülü konuşma destekleniyor mu?	C		
TO_3	Görüntülü konferans destekleniyor mu?			A
TO_4	Sesli konferans destekleniyor mu?			A
TO_5	HD görüntü codecleri destekleniyor mu?		B	
TO_6	Video Quality negotiation destekleniyor mu?			A
TO_7	Çağrı tutma destekleniyor mu?		B	
TO_8	Çağrı aktarma destekleniyor mu?			A
TO_9	Birebir mesajlaşma destekleniyor mu?	C		
TO_10	Grup mesajlaşma destekleniyor mu?	C		
TO_11	Çevrimdışı (Offline) mesajlaşma destekleniyor mu?	C		
TO_12	İletim/Okundu bilgisi raporu destekleniyor mu?	C		
TO_13	Push notification destekleniyor mu?	C		
TO_14	Kaybolan mesaj (disappearing messages) destekleniyor mu?		B	
TO_15	Gönderilen mesaj, medya, ses dosyaları gönderen tarafından alıcıdan silinebiliyor mu?	C		
TO_16	Fotograf / video paylaşımı destekleniyor mu?	C		
TO_17	Doküman paylaşımı destekleniyor mu?	C		
TO_18	Kontak paylaşımı destekleniyor mu?	C		
TO_19	Konum paylaşımı destekleniyor mu?	C		
TO_20	Canlı konum paylaşımı destekleniyor mu?		B	
TO_21	Duyuru/toplu mesaj destekleniyor mu?	C		
TO_22	Mesajlaşma kanalları sessize alınabiliyor mu?	C		
TO_23	Kullanıcı mesajlarının yedeğini uygulama sunucusunda saklayabiliyor mu ?	C		
TO_24	Mesajlar üzerinde arama yapılabiliyor mu?	C		
TO_25	Kullanıcı engelleme özelliği var mı?	C		
TO_26	Grup mesajlaşmada rol yönetimi var mı?	C		
TO_27	IOS veya ANDROID desteği var mı?	C		
TO_28	PC desteği veya Web tarayıcı desteği var mı?		B	
TO_29	Tek kullanımlık şifreler (OTP) uygulama üzerinden gönderilebiliyor mu ?			A

TO_30	Kişi listesi özelliği var mı?	C		
TO_31	Yönetim paneli bulunuyor mu?	C		
TO_32	Sistem yöneticisi tarafından grup oluşturma/silme aksiyonları alınabiliyor mu?		B	
TO_33	Sistem yöneticisi tarafından kullanıcı bloklama yapılabiliyor mu?	C		
TO_34	Kullanıcının izni alınmadan herhangi bir gruba dahil edilmemesi sağlanabiliyor mu?			A
TO_35	Uygulama özelinde bildirim ayarları değiştirilebiliyor mu?	C		
TO_36	Kullanıcı özelinde bildirim ayarları değiştirilebiliyor mu?		B	
TO_37	Kuruma özel kurulum (on premise installation) yapılabiliyor mu?	C		
TO_38	Kullanıcılara yönelik uygulama ile ilgili yardım menüsü bulunuyor mu?	C		
TO_39	Güvenilir ortamda yapılan mesajların ekran görüntüsü, ekran video kaydı alınmasının engellenmesi işlemi opsiyonel olarak sunulabiliyor mu? (android)			A
TO_40	Sesli ve Görüntülü arama sırasında mesaj yollama, dosya ve yazı paylaşımı yapılabiliyor mu?			A
TO_41	Web ten sesli ve görüntülü görüşme yapılabiliyor mu?			A
PK	**4- Performans / Kapasite**			
PK_1	Toplam sisteme kayıt olabilecek kullanıcı sayısı (minumum 10.000)	C		
PK_2	Toplam aynı anda aktif kullanıcı sayısı (minumum 1.000)	C		
PK_3	Anlık (concurrent) atılan mesaj kapasitesi (teslim ve okundu raporlarını da içerecek şekilde) (saniyede minumum 1.000)	C		
PK_4	Günlük atılan mesaj kapasitesi (teslim ve okundu raporlarını da içerecek şekilde) (minumum 2.000.000 mesaj)	C		
PK_5	Anlık atılan medya ve dosya kapasitesi (saniyede 200KB ortalama ile minumum 500 medya)	C		
PK_6	Bir mesajın uçtan uca iletilme süresi (Servisler dahil) (Ortalama Maximum 3 sn) (FCM ve APNS'nin vb. servislerin sağlıklı çalıştığı ortamlar için)	C		
PK_7	Aynı anda iki kişi arasında görüşme sayısı (minumum 100 görüşme)	C		
PK_8	Günlük görüşme sayısı (minumum 1.000 görüşme)	C		
PK_9	İki uygulama açıkken minumum çağrının kurulabilme süresi (ortalama maximum 3 sn)	C		
SR	**5- Sorgulama ve Raporlama**			
SR_1	Raporlama modülü bünyesinde ön tanımlı raporlar bulunuyor mu? (en az kullanıcı sayısı, aktif kullanıcı sayısı, pasif kullanıcı sayısı vb.)	C		
SR_2	Arayüzde yapılan sorguların sonuçlarını pdf, doc, docx, xls, xlsx, csv, html formatında dışarı aktarılabiliyor mu?	C		
SR_3	Toplanan kayıtlardan olay incelemesi amacıyla IP adresi, profil sorgusu yapılabiliyor mu?	C		
UD	**6- Ürün Dokümantasyonu**			

UD_1	Türkçe ve İngilizce doküman desteği var mıdır?	C		
UD_2	Kurulum, ürün özellikleri, destek metodlarına, uygulama altyapısına ilişkin bilgileri gösteren bir doküman yer alıyor mu?	C		
RU	**7- Regülasyonlara Uyum**			
RU_1	Ulusal çerçeveler içerisinde bağlayıcı kanun hükümlerine uyumluluk sağlıyor mu? (KVKK vb.)	C		
RU_2	Uluslararası anlaşmalar dahilinde uyulması gereken standartlar karşılanıyor mu? (GDPR vb.)			A