

HESAP EKSTRESİ WEB SERVİS ENTEGRASYONU BAŞVURU FORMU

MÜŞTERİ	
MÜŞTERİ İSMİ	
MÜŞTERİ NO	
MÜŞTERİ VKN/TCKN	

WEB SERVİS KULLANILACAK HESAPLAR	
TÜM HESAPLARIM	☐
BELİRTTİĞİM HESAPLAR	

ERİŞİM YETKİLİSİ BİLGİLERİ	
IP ADRESİ	62.244.219.12 - 62.244.219.32 - 185.157.42.138
YETKİLİ ADI	
YETKİLİ TCKN	
YETKİLİ GSM NO	
YETKİLİ E-POSTA	
YETKİLİ DOĞUM TARİHİ	

Hesaba ilişkin her türlü işlemi yapma yetkisi ve her türlü kontrol yetkisi tarafımıza ait olmak üzere ve ayrıca hesaba ilişkin bu bilgilerin elektronik ortamda aktarıldığının bilincinde olarak, Bankanız Web Servis Uygulamasından yararlanmak için yukarıda belirtilen hesabımıza/hesaplarımıza ait hesap hareketlerinin POLYNOM TEKNOLOJİ BİLGİSAYAR YAZILIMLARI BİLİŞİM DANIŞMANLIK VE SANAYİ A.Ş.'ne web servis entegrasyonu kurularak paylaşılmasını rica ederiz. Bu talebimiz kapsamında işbu Formun arka sayfasındaki Web Servis Güvenliği Bilgilendirmesini okuduğumuzu ve bu bilgilendirmedeki güvenlik tedbirlerinin tarafımızca alınacağını, aksi durumda ortaya çıkacak her türlü sonuçtan da tarafımızın sorumlu olacağını kabul, beyan ve taahhüt etmekteyiz./...../.....

MÜŞTERİ



Web Servis Güvenliđi Bilgilendirmesi

Bankamızın Web Servis-API hizmetlerini hizmetlerin kullanımında güvenlik için dikkat etmeniz gereken hususlar şöyledir:

- Web servislere erişimin sadece yetkilendirilmiş kaynaklar tarafından yapılması sağlanmalıdır. Bu kapsamda gerekli bileşenler kullanılmalı (Switch, Router, Firewall, v.b.) ve gerekli güvenlik konfigürasyonları yapılmalıdır.
- Web servis iletişimi güvenli iletişim protokolü olan TLS kullanılarak sağlanmalıdır. Web servis sağlayıcısı iletişimi zamanı dolmamış, iptal edilmemiş ve yürürlükten kaldırılmamış sunucu sertifikaları ile sağlamalıdır.
- Web servislere erişim ve ilgili fonksiyonların kullanımı daha önceden tanımlanmış Doğrulama (Validation) ve Yetkilendirme (Authentication) mekanizması tarafından kontrol edilmeli ve yetkisiz erişimler engellenmelidir.
- Web servise iletişim kapsamında çeşitli filtreler uygulanmalıdır. Bu filtreler aynı anda veya birbirinin yerine kullanılabilir. İki tip filtreleme kullanılabilir: Zaman Filtresi ve IP Filtresi.
 - Zaman filtresi, sunulan web servise ve/veya fonksiyonuna sadece o fonksiyon tarafından belirlenen zaman dilimlerinde erişimi sağlamalıdır.
 - IP filtresi, sunulan web servise sadece belirlenen IP adres bloklarından erişimi sağlamalıdır.
- Web servisi kapsamında kullanılan mesajların belirlenen XML şemasına uygun olduğu denetlenmelidir. Schema validasyonundan geçemeyen istekler kabul edilmemelidir.
- Web servislerinin yoğun kullanımı durumunda hizmetin erişilebilirliğinin sağlanması amacıyla gerekli alt yapı kurulu olmalıdır. Gelen isteklerin yükü dengelenmeli ve web servislerine erişim sürekli olarak sağlanmalıdır.
- Web servisleri kapsamında giden ve gelen XML mesajların büyüklüğü için bir mesaj kapasitesi kullanılan web servis fonksiyonları bazında belirlenmelidir. Gelen web servis istekleri eđer mesaj kapasitesini aşıyorsa reddedilmeli, gönderilecek mesajlar kapasite aşımını önleyecek şekilde gönderilmelidir.
- Web servisleri kapsamında giden, gelen mesajlar herhangi bir zararlı yazılım ve kötü niyetli kod parçacığına karşı taranmalı ve zararlı içerik taşıyan istekler reddedilmelidir.
- Web servislerine yapılan her türlü erişim (erişim yapan IP, zaman, erişim yapılan fonksiyon, erişimi gerçekleştiren kullanıcı) gibi bilgilerle kayıt altına alınmalıdır.
- Web servisleri sürekli kontrol edilerek deđişen teknoloji ve ihtiyaçlara göre gerekli güvenlik güncellemeleri yapılmalıdır. Alınan kayıtlar incelenmeli ve varsa yetkisiz erişimler tespit edilerek güvenlik önlemleri artırılmalıdır. Ayrıca her yeni eklenen web servis veya fonksiyonun gerekli yetkilendirmeleri ve her yeni eklenen kullanıcının tanımları kontrol edilmelidir. Benzer şekilde iptal edilen fonksiyonlar ve iptal edilen kullanıcılara göre güvenlik önlemleri güncellenmelidir.
- Kullanıcı adı-şifreler yalnızca size özeldir, açık biçimde herhangi bir yere kaydedilmemeli ve destek kapsamında olsa dahi 3. Taraflarla paylaşılmamalıdır. Açığa çıkmış kullanıcı adı-şifre olduğu fark edilirse Bankamız ile derhal iletişime geçilmelidir.

