



Sigorta
Bilgi ve Gözetim
Merkezi

SBM Online SBM Authenticator Kullanım Kılavuzu

Versiyon [1.0]
[04.2023]

İÇİNDEKİLER

1	REVİZYON TARİHÇESİ	3
1.1	Değişiklik Tarihçesi	3
2	AMAÇ	3
3	KAPSAM	3
4	SBM Online İki Faktörlü Doğrulama Süreci	3
4.1	SBM Authenticator Mobil Uygulama Kurulumu	3
4.2	SBM Online Mobil Cihaz Tanımlama – İki Faktörlü Doğrulama Adımları	3
4.3	Mobil Cihaz Tanımlama Sürecinin Tekrarlanmasını Gerektiren Durumlar	7
4.4	SBM Authenticator Uygulamasını Kullanırken Dikkat Edilmesi Gerekenler	8

1 REVİZYON TARİHÇESİ

1.1 Değişiklik Tarihçesi

Versiyon	Tarih	Hazırlayan	Açıklama	Onaylayan
1.0	04.04.2023		Kılavuz oluşturuldu.	

2 AMAÇ

Bu kılavuz, SBM Online platformu ortamlarında uygulanacak iki faktörlü doğrulama sürecinin işleyişi hakkında platform kullanıcılarını bilgilendirmek amacıyla hazırlanmıştır.

3 KAPSAM

SBM Online platformu ortamlarında uygulanacak iki faktörlü doğrulama süreci ve süreçte kullanılacak SBM Authenticator mobil uygulamasına ilişkin bilgiler kılavuz kapsamında yer almaktadır.

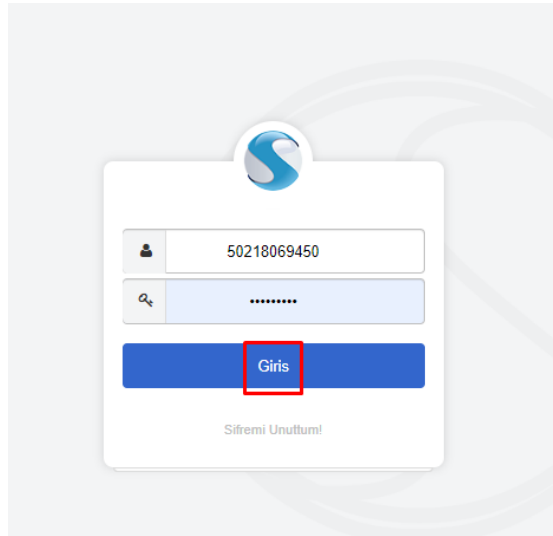
4 SBM Online İki Faktörlü Doğrulama Süreci

4.1 SBM Authenticator Mobil Uygulama Kurulumu

SBM Online platformunda iki faktörlü doğrulama sürecini tamamlayabilmek adına platforma giriş yapacak kullanıcılar mobil cihazlarının işletim sistemine göre Google Play ya da Apple App Store üzerinden “SBM Authenticator” uygulamasını mobil cihazlarına kurmalıdır.

4.2 SBM Online Mobil Cihaz Tanımlama – İki Faktörlü Doğrulama Adımları

- 1) Kullanıcıların <https://online.sbm.org.tr/sbm-admin/cweb/public/home.sbm> linki ile Resim1’de yer alan SBM Online platformu login ekranına erişip login bilgilerini girerek “Giriş” butonunu seçmeleri beklenmektedir.

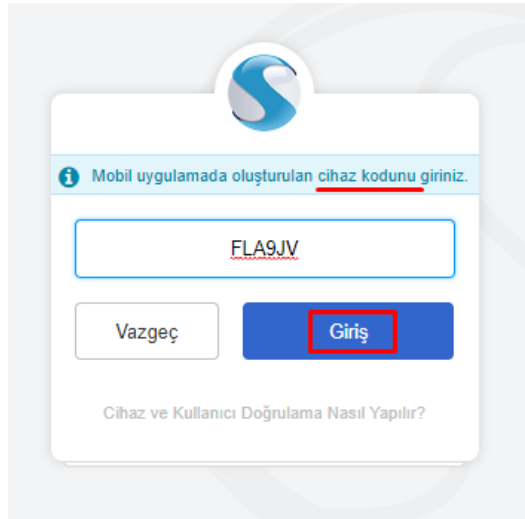


Resim 1

- 2) Login bilgilerini doğru bir şekilde girdikten sonra bu adımda mobil cihaz doğrulaması yapılacaktır. Mobil cihazınızda “SBM Authenticator” uygulamasını çalıştırdıktan sonra Resim 2’de yer alan mobil uygulama üzerindeki “Cihaz ID” değeri, Resim 3’de SBM Online’da açılan ekran üzerindeki forma yazılıp giriş butonu seçilerek mobil cihaz doğrulama adımı tamamlanacaktır.



Resim 2



Resim 3

- 3) Bu aşamada SBM Online ekranında Resim 4'te görülen karekod SBM Authenticator mobil uygulamasında yer alan "QR Kodunu Tarayın" (Resim 5) seçeneği ile taratılır.

i Mobil uygulama ile QR kodu okutunuz ve mobil uygulamada oluşan kodu giriniz.
Güvenlik kodu giriş yapmadan önce kullanıcı adınızın altında yer alan Cihaz ID'nin doğruluğundan emin olunuz.



502*****50

FLA9JV

Güvenlik Kodu

Vazgeç Giriş

Cihaz ve Kullanıcı Doğrulama Nasıl Yapılır?

Resim 4



Hesap Oluşturma
Hesap oluşturma işlemi için size iletilen QR kodunu tarayın

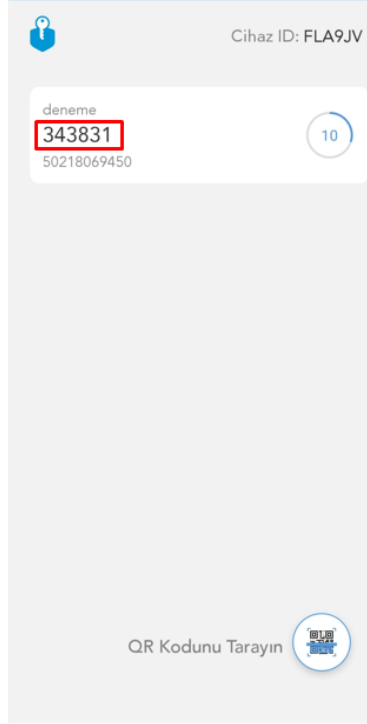
Cihaz ID
FLA9JV

QR Kodunu Tarayın

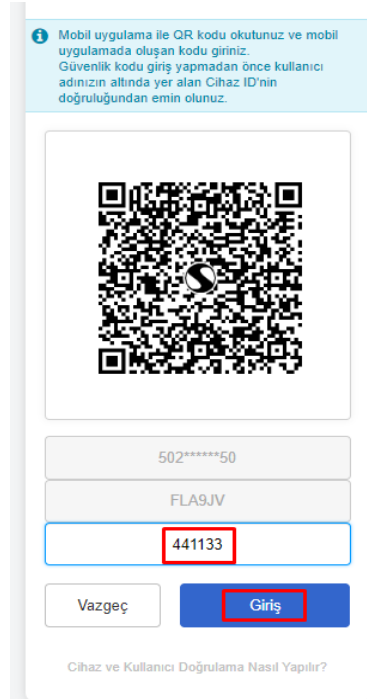
SBM Authenticator, Sigorta Bilgi ve Gözetim Merkezi tarafından geliştirilmiştir.

Resim 5

- 4) Mobil cihaz kodunun doğruluğu önem arz etmektedir ve mobil cihaz kodu doğru girilmeden QR kod okutulması durumunda “Geçersiz QR kod” hatası alınacaktır. Eğer mobil cihaz kodu doğruysa SBM Authenticator uygulamasında güvenlik kodu oluşacaktır (Resim 6). Oluşan süreli güvenlik kodu SBM Online ekranındaki “Güvenlik Kodu” alanına girilip, “Giriş” butonu (Resim 7) seçilerek iki faktörlü doğrulama süreci tamamlanmış olur.



Resim 6



Resim 7

- 5) İki faktörlü doğrulama süreci tamamlandıktan sonra kullanıcılar birinci maddede yer alan SBM Authenticator uygulamasında oluşmuş olan güvenlik kodunu her login işleminde girerek yeniden mobil cihaz tanımlaması ve QR kod okutma sürecinin tekrarlanmasına gerek kalmadan doğrulamayı tamamlayabilirler (Resim 8). Mobil cihaz tanımlama sürecinin tekrarlanmasını gerektiren durumlar 4.3 bölümünde belirtilmiştir.

Resim 8

- 6) Sisteme kayıtlı kullanıcı için 2 kere cihaz tanımlama ve QR kod okutma işlemleri yapılması sonucu 2 farklı kod oluşursa sistem ilk kodu kabul etmez. En son oluşturulan kod ile giriş yapılmalıdır.
- 7) Kullanıcılar işbu kılavuzunu Resim4 ve Resim 7’de yer alan “Cihaz ve Kullanıcı Doğrulama Nasıl Yapılır?” butonunu seçerek görüntüleyebilirler.

4.3 Mobil Cihaz Tanımlama Sürecinin Tekrarlanmasını Gerektiren Durumlar

Aşağıda yer alan dört durum için 4.2 bölümünde yer alan mobil cihaz tanımlama sürecinin tekrarlanması gerekmektedir:

- 1) Kullanıcının şifresini yenilemesi/değiřtirmesi.
- 2) Kullanıcının 4.2 bölümü birinci adımındaki login işleminde üç kez üst üste şifresini yanlış girerek kullanıcının kilitlenmesi.
- 3) Kullanıcının 4.2 bölümü beşinci adımında yer alan güvenlik kodu girişini üst üste beş kez yanlış yapması.
- 4) Kullanıcının mobil cihaz değışikliğı yapması.

4.4 SBM Authenticator Uygulamasını Kullanırken Dikkat Edilmesi Gerekenler

- 1)** Kullandığınız cihazın QR kodu okuyabildiğinden emin olunuz.
- 2)** QR kodun okunabilmesi için kamera netliği ve yansıma olmaması gibi durumlara lütfen dikkat ediniz.
- 3)** SBM Online Authenticator uygulaması JailBreak kullanılan cihazlarda çalışmamaktadır.