# Denizbank PROD API Entegrasyonu

Dijital imzalama yapısı, API'de gerçekleştirilen işlemlerin ve taşınan verilerin bütünlük ve inkâr edilemezliğini sağlamak amacıyla kurgulanmıştır.

HTTP isteğinin gövdesinin hash fonksiyonu (SHA256) ile özetinin alınması, elde edilen özetin RSA algoritması kullanılarak imzalanması ve oluşan JWS'nin HTTP isteğinin başlığında gönderilmesi gerekmektedir.

Bu kapsamda imzalama akışı aşağıdaki gibi olmalıdır:

### 1. Sertifikaların Oluşturulması

Öncelikle public ve private anahtarlar oluşturmalıdır. Bu anahtarları oluşturmak için aşağıda *openssl* kullanılarak oluşturma örneği paylaşılmıştır.

#### Private anahtarın oluşturulması

openssl genrsa -out private.pem 2048

Java ile geliştirilen uygulamalar için sertifikanın PCKS8 formatına dönüştürülmesi gerekmektedir. openssl pkcs8 -topk8 -inform PEM -in private.pem -out private\_key.pem –nocrypt

Not: Sertifikalar 2048 bit veya üzeri olmalıdır.

#### Public anahtarın oluşturulması

openssl rsa -in private.pem -pubout -outform PEM -out public\_key.pem

Private anahtar mesajı imzalamak için kullanılacak olup, public anahtar ise mesajı doğrulamak amacıyla banka tarafından kullanılacaktır. Bu sebeple oluşturulan public sertifikanın Denizbank İnternet Bankacılığı üzerinden yüklenmesi gerekmektedir.

### 2. Sertifikaların Yüklenmesi

Denizbank Internet Bankacılığında Ayarlar → API menüsünden Sertifika Ekle / Düzenle ekranına giriş yapılıp, sertifika yüklenecek uygulama (müşterinin adına daha önceden her AppKeye özel oluşturulmuş olan requestlerde kullanılan Channel parametresi) seçilerek imzalama için kullanılacak JWS algoritması Algoritma menüsünden seçildikten sonra openssl ile oluşturulmuş public anahtarın girilmesi gerekmektedir. Var olan sertifikanın görüntülenmesi/güncellenmesi yine aynı ekran üzerinden yapılabilmektedir.

**Not:** Her farklı appkey e sahip uygulama kendi sertifikasını üretip internet bankacılığı ekranından siteme yüklemesi gerekmektedir.

0	Ana Sayfa		8	😂 💼 🖉 🗸 🖉 DenizBank 🕸				( <sup>1</sup> ) Çıkış		
Inte C	rnet Şube'de Ara Daşvurular	Q	< Ana Sayfa		Sertifika Ekle / Düzenle				(	😚 Favorilerim'e Ekle
•	Tüm İşlemler									
Θ	Ayarlar	~			Sertifika Bilgileri					
	Bilgi Güncelle				Uygulama Adı	Algoritma	Son Kullanma Tarih	ni		
	Şifre / Parola									
	lletişim ve Finansal Veri Tercihleri					RS512	19.01.2025	6	2	
	Güvenlik Kısıtları									
	Favorilerim'i Düzenle	1	r.					Yeni Sertif	ika Ekle	
	Yetki İşlemleri							1.1		
	Bakiye / Hareket Gizle									
	e-Devlet Girişi									
	API	^								
	API Yetkilendirme									
	APLizie / İptal Et Sertifika Ekle / Düzenle									
0	Bize Ulaşın									
0	Hızlı Fx		M ENBD	2024 DenizBank.	Tüm hakları saklıdır. <mark>DocQ9MQjGg</mark>	zDAKr5pyMR - 20240216.2025	(e	🥑 e-Devlet'e Giriş	OB20 222 0 800	Güvenlik ve Yardım

## Sertifika Yükleme – 1

0	Ana Sayfa		8	Sertifika Bilgilerini Ekle	Kapat 🛞	( <sup>1</sup> ) Çıkış
Interr	net Şube'de Ara	Q				
9	Daşvülulai		< Ana Sayfa	Sertifika hilgilerini hu alandan eklevehilirsiniz		(🖄 Favorilerim'e Ekle
•	Tüm İşlemler					
Θ	Ayarlar	^		Uygulama Adı		
	Bilgi Güncelle			Seçiniz 🗸		
	Şifre / Parola					
	lletişim ve Finansal Veri Tercihleri			Algoritma		2
	Güvenlik Kısıtları			Seçiniz		
	Favorilerim'i Düzenle			Sertifika		ertifika Ekle
	Yetki İşlemleri					
	Bakiye / Hareket Gizle					
	e-Devlet Girişi					
	API	~				
	API Yetkilendirme					
	API izle / iptal Et					
	Sertifika Ekle / Duzenie					
0	Bize Ulaşın			Kaydet		
0	Hızlı Fx		M ENBD		-	iriş 🚯 0850 222 0 800 🔘 Güvenlik ve Yardım

Sertifika Yükleme – 2

Ana Sayfa		Sertifika Bilgilerini Düzenle		Kapat (×)		( <sup> </sup> ) Çıkış	
Inte	rnet Şube'de Ara Daşvurular	Q	< Ana Sayfa				💮 Favorilerim'e Ekle
0	Tum İşlemler			Sertifika bilgilerini bu alandan düzenleyebilirsiniz.		-	
0	Ayarlar	^		Uygulama Adı			
	Şifre / Parola					-	
	lletişim ve Finansal Veri Tercihleri			Algoritma		2	
	Güvenlik Kısıtları			RS512 V			
	Favorilerim'i Düzenle			Sertifika		ertifika Ekle	
	Yetki İşlemleri Bakiye / Hareket Gizle e-Devlet Girişi API API Yetkilendirme API İzle / İptal Et	^		MIIBIJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAztQF D992WP8OIMPyr2x52S0Ilvki5w8WiJ6Ih+vfWh9tqgz4eeBP4My Bp6m5yvobEv899pIDqag03e/9L8UQfBwRyzhbacACAVqEZMc aAJof5KH5UaXwueq2V+EZKmtpVgIAnTESNRXHdtRwCrbNC7P F820tVUJYk0gw57m3034Fg0Utqq7Cqdf3GL546g5Hh+WyD EwrCPAHHoDbG38toEMI6AVMo80vEvMIMLPo7Iz7b2doLUSqI5			
	Sertifika Ekle / Düzenle						
0	Bize Ulaşın			Değişiklikleri Kaydet			
0	Hızlı Fx		M ENBD			iriş 🧿 0850 222 0 800	Güvenlik ve Yardım

Sertifika Görüntüleme / Güncelleme

## 3. İsteklere Zaman Damgasının Eklenmesi

HTTP isteğinin gövdesinde RequestDate parametresine istek tarihinin eklenmesi gerekmektedir.

```
{
    "Header": {
        "AppKey": "{{AppKey}}",
        "Channel": "{{Channel}}",
        "ChannelSessionId": "5CE7303B-9C0E-4628-A9E7-3F34D28FEC8D",
        "ChannelRequestId": "525F2F2D-B852-4B46-9FC3-9B765BC86AAA",
        "RequestDate": "2024-01-17T09:32:52.7086442+03:00"
    },
    "Parameters": [
        {
            ...
        }
    ]
}
```

### 4. İstek Gövdesinin İmzalanması

Mesaj imzalama gerektiren her API isteği için oluşturulan JWS'nin HTTP isteğinin başlığında **Signature** alanında göndermesi gerekmektedir.

Requestin oluşturulması ve imzalanması aşamaları şu şekildedir;

- 1. Request body de headera "RequestDate" alanı eklenecek
- 2. Oluşan request body değeri serialize edilecek
- 3. Serialize edilen request body UTF8 encoding ile hashlenecek
- 4. Hash sonrası base64stringe dönüştürülecek
- 5. Private key değeri formbase64stringe dönüştürülür
- 6. Oluşan değer RSA ile provider create edilir

- 7. Oluşan provider importPkcs8Privatekey ile dönüştürülen formbase64string değeri out edilir
- 8. 4.adım sonucunda oluşan değer provider JwsAlgorithm.RS256 ile jwt encode edilir. (Not: buradaki RS256 değeri internet bankacılığı ara yüzünden sertifika yüklenirken seçilen algoritma değerine göre değiştirilmelidir. Ör. Algoritma RS512 seçildiyse JwsAlgorithm.RS512 ile jwt encode edilecektir)
- 9. İmzalanan bu değer request header da signature alanında gönderilir.

**API PROD Endpoint:** https://apigw.denizbank.com/api/v2/{ApiName}