Denizbank UAT 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 özeti alınacaktır. Elde edilen özet, RSA algoritması kullanılarak imzalanacak ve JWS elde edilecektir.

Bu kapsamda imzalama akışı aşağıdaki gibi olmalıdır:

1. **Private Sertifikanın Alınması**

UAT ortamımız, API'lerimize olan bağlantıyı test etmenizi sağlar. UAT ortamında banka tarafından iletilecek private sertifika ile isteklerin imzalanması gerekmektedir.

UAT sertifikası RSA-2048 bit ile oluşturulmuştur ve imzalama algoritması SHA-256'dır.

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDO1AUP31lY/w6I
w/K/bFJlLSUi+SLnAFaPqWH699aH22qDPh54E/gzIGnqbnK+hsS8H32mUOpqA7d7
/0vxRB8HBHLOFtpwAIBWqMRkxxoAmh/qQflRpfC56plj4Rkqa2liAgCdMTk1Fcd3
RHAKts0Ls8XzY61hSNiQ6DBLubcPfgeCLQt+qrs6p12NKovn4Grk8fFalkXKAI/g
cekOEbfy2gQwnoBgyjzTETEwws+juXPtvZ2otRKonkud8XUrOtbkg2oVi1onu4hb
qbuf8GxgFPAP+Hrlm6HoIrUwwIO4+4WBEztNNKytL2L0ARwSiod1uyvEba6Fqokp
kif0jSn/AgMBAAECggEAFVy+vRnzj4agiK28d9sHU53rFQaofTWCu0nibdqFVPjr
smyLFxnw687wQZ9wyI8A6PFTuAbpf1Os8ui2fk/r6HyklvcnTqQunUTHLCWIYQGK
RFbWGoHKMFmzyCYqxD/d3ZqZV6MK5pm+RWpTLDgfS5Mg4feso7yzaZwhyOCAsN/C
68p9ymNsB89qStRcjXIyJYXqpN0y7+3yCyTthkbO4RIzihAqtYZWg9sUtuDmEW3U
lMJMd6MRe1lhCKUg1+ku3fmqOVi4LY0aStlnuxp7l6/6BKlVaLBIQuswbMsT+VIA
tIHfslBpAt7BvsHDDoPEsr3BRDbLAQRYxfemkeIQEQKBgQDyXxoD6z05chdNEIQm
wflFNEMoep2Qy7xf1XqVLTgIs6kUMhABbPpWCHu5M67di9CTNRiEZUsWecj5+lKl
rusncrCp+xBtcAU6lY74VwBL+17zAUo0gGS1WdDbAg8eAY3vQn8pFmeGZZnfODxd
LEiBM1DFCGnhfxwSyA63a0OzVwKBgQDadUc8fWimdaVG+btohXHFX+XhnfuDXoV3
EH0lPTsQVYBpMh2dB9EcORHfijJuIP19MinWIt527d1cJuxlx1gW81W2Mb3FCOZg
1jBzA0Q18a4rxzBLsHL7tsT/45ovWtjN24uN1rxiGXP7txj6CeP1mX8p9a/yZf/k
FVQ4d7b9mQKBgQDCx2Lk21vsmp/XMvrBGwn0b7e5BDE0eEb+zVUiJaDufVPYAxOR
0b6s/UxQ3hQdv4rzgqwdWjop6d1155IbzKL2pNkNAdOF34yUNDUdpu16Ip1/tP2p
i7VjeLa8Cr+TYbRrH4mJv5ObEnPCTDNWvYvXKSIz9jsBGWG6RkRtayqRKQKBgQCK
pBNpmE1qFw+lU6hUVRw3Hv1Nim2smbgqMBS8JXfujdTI7j1NA0D6oF1veM04h0dY
xRU4CTkWUS9C5JDypuiI6DVlQ3wkJ9nNayGkXFZVxeO7dNZ5sqnGhd/QZincE9O0
EbknczhrKawp+7GmPdCmdZv2jS30sDcOEVs52wAPQQKBgGPBQlm8uEieLwTW5g3V
GbpQRWJh1uJgDdTJ6ntCxj7l1nE2fWURcxLzt0bEyRfXraE72jEq3MHBic/8WvxV
fjTaS6L5IT/kQJD+b4cVwqzicojA0KhtpYEbTAGKnqxOjDSQMtZ/WUHSGjA1ejl9
idFNSgQNauMBiwkVUQ8Dga6I
-----END PRIVATE KEY-----
```

2. 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": [
        {
            ...
        }
    ]
}
```

3. İstek Gövdesinin İmzalanması

API tüketicilerinin, mesaj imzalama gerektiren her API isteğinin HTTP gövdesini (request body) private key ile şifreleyerek imza bilgisini oluşturması ve bu imza verisini, göndereceği mesajın istek başlığında (request header) yer alan *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

İmzalanan bu değer request header da signature alanında gönderilir.

API UAT Endpoint: https://ssgtest.denizbank.com:9443/apiuatv2/{ApiName}