Bankacılık Düzenleme ve Denetleme Kurumundan:

Görüşlerinizi bsmevzuat@bddk.org.tr adresine e-posta ile iletebilirsiniz.

T.C.
BANKACILIK DÜZENLEME VE DENETLEME KURUMU

Sayı :
Konu : Elektronik Bankacılık Hizmetlerinde ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasında Kimlik Doğrulama ve İşlem Güvenliği için Sağlanması Gereken Kriterler Hk.

GENELGE
(2022/2)

Bilindiği üzere, 15/03/2020 tarihli ve 31069 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliğin (BSEBY) 34 ve 35 inci maddelerinde elektronik bankacılık hizmet kanallarında kimlik doğrulama ve işlem güvenliğinin nasıl gerçekleştirilmesi gerektiği ve bu kanallar üzerinden gerçekleştirilecek işlemler için hem banka hem de müşteriler için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikler kullanılması gerektiği düzenlenmekte olup, BSEBY'nin 38 inci ve 39 uncu maddelerinde ise internet bankacılığı ve mobil bankacılık dağıtım kanalları özelinde bu hususlara ilişkin ilave hükümlere yer verilmiştir.

Diğer taraftan, 01/04/2021 tarihli ve 31441 sayılı Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmeliğin (UKTY) 12 nci maddesinin ikinci fıkrasında ise BSEBY'nin 38 ve 39 uncu maddelerine atıfta bulunulmak suretiyle aşağıdaki hükümlere yer verilmiştir:

"(2) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılmasını ya da şubeler aracılığıyla müşteri kimliğinin yüz yüze tespit edilmesini müteakiben, ***mesafeli olsun olmasın, müşterilerce gerçekleştirilmek istenen işlemlere yönelik olarak bir bilişim veya haberleşme cihazı üzerinden yazılı şeklin yerine geçecek nitelikte bir sözleşme ilişkisi kurulabilmesi için****;*

a) ***Söz konusu sözleşmenin bütün şartlarının, müşterinin okuyabileceği şekilde internet bankacılığı ya da mobil bankacılık dağıtım kanalları üzerinden müşteriye iletilmesi****,*

b) (a) bendine göre müşteriye iletilen sözleşme ve bu sözleşme ile birlikte müşterinin ***sözleşmeyi kuran irade beyanının, BSEBY'nin 38 inci maddesinin üçüncü fıkrası ile 39 uncu maddesinin birinci fıkrasında belirtilen müşteriye özgü şifreleme gizli anahtarı ile imzalanarak bankaya iletilmesi****,*

c) ***(a) bendine göre iletilen sözleşmede müşteriye sözleşme içeriği olarak hangi bilgiler gösterilmiş ise (b) bendine göre müşteri tarafından yalnızca o bilgilerin imzalanmasının sağlanması****,*

şarttır."

Ayrıca, 29/12/2021 tarihli ve 31704 sayılı Resmi Gazete'de yayımlanan Dijital Bankaların Faaliyet Esasları ile Servis Modeli Bankacılığı Hakkında Yönetmeliğin (DBY) 13 üncü maddesinin dördüncü ve beşinci fıkralarında da aşağıdaki hükümlere yer verilmiştir:

(4) Servis bankasının arayüz sağlayıcının müşterisine bankacılık hizmetleri sunabilmesi için söz konusu müşteri ile servis bankası arasında Kanunun 76 ncı maddesi uyarınca sözleşme ilişkisinin kurulması gereklidir. ***Söz konusu sözleşme ilişkisinin elektronik ortamda kurulması halinde, sürecin UKTY'ye uygun olarak yürütülmesi ve müşteri kimliğinin UKTY'ye uygun olarak servis bankası tarafından tespit edilmesi zorunludur. Servis bankası ile müşteri arasındaki sözleşme ilişkisi kurulması sürecinin arayüz sağlayıcının mobil uygulaması ya da internet tarayıcısı temelli arayüzü üzerinden başlatılıp yine bu hizmet kanalları üzerinden tamamlanması halinde, arayüz sağlayıcının söz konusu hizmet kanallarının BSEBY'de yer verilen güvenlik kriterlerine uygun olması ve müşteriye sözleşme içeriği olarak hangi bilgiler gösterilmiş ise müşteri tarafından yalnızca o bilgilerin onaylanmasının sağlanması konusunda güvence sağlayacak nitelikte olması servis bankasının sorumluluğundadır.***

(5) Müşterinin servis bankasının sunduğu hizmetlere erişmede kullandığı ***arayüz sağlayıcının mobil uygulaması ya da internet tarayıcısı temelli arayüzünün, BSEBY'nin üçüncü kısmında elektronik bankacılık hizmetlerine ilişkin yer verilen kimlik doğrulama ve işlem güvenliği yükümlülüklerine uygun olmasını sağlamak konusunda arayüz sağlayıcı ve servis bankası müteselsilen sorumludurlar.*** *Servis bankası, bu yükümlülükleri yerine getirmeyen ya da sistemleri bu yükümlülükleri yerine getirme konusunda yetersiz olan arayüz sağlayıcılara servis modeli bankacılığı hizmeti sunamaz ve bunlardan destek hizmeti alamaz.*

Bu kapsamda, söz konusu düzenleme hükümlerinin işlem güvenliğinden ödün verilmeksizin yeknesak bir şekilde nasıl uygulanacağı konusuna açıklık getirmek ve söz konusu hükümler konusunda yaşanabilecek tereddütleri gidermek amacıyla, bu hükümlerin uygulanmasında, 5411 sayılı Bankacılık Kanununun 76 ncı maddesinin ikinci fıkrası ile 93 üncü maddesi çerçevesinde alınan XX tarihli ve XXXX sayılı Kurul Kararı ile onaylanan ekte yer alan açıklamaların dikkate alınması gerekmektedir.

Tebliğ olunur.

Mehmet Ali AKBEN
Başkan

Ek: Açıklamalar

ELEKTRONİK BANKACILIK HİZMETLERİNDE VE ELEKTRONİK ORTAMDA SÖZLEŞME İLİŞKİSİNİN KURULMASINDA KİMLİK DOĞRULAMA VE İŞLEM GÜVENLİĞİ İÇİN SAĞLANMASI GEREKEN KRİTERLER HAKKINDA EK AÇIKLAMALAR

1. Müşteriye Özgü Şifreleme Gizli Anahtarının Kullanılması ve İşlem İmzalama *(BSEBY Madde 34-38-39):*

Bilindiği üzere BSEBY'nin 38 inci maddesinin üçüncü fıkrası ile 39 uncu maddesinin birinci fıkrası aşağıdaki hükümleri amirdir:

(3) İnternet bankacılığı dağıtım kanalında 34 üncü maddenin birinci fıkrasına göre gerçekleştirilecek kimlik doğrulama işlemi için ***müşteriye atanmış bir şifreleme gizli anahtarı ile imzalanacak şekilde tek kullanımlık bir doğrulama kodu üretilir****. Doğrulama kodu aracılığıyla 34 üncü maddenin birinci fıkrasında belirtilen kimlik doğrulama unsurlarından hiçbiri hakkında bilgi edinilememesi, bilinen bir doğrulama kodu ile geçerli başka doğrulama kodlarının türetilememesi, doğrulama kodlarının taklit edilememesi sağlanır.* ***Finansal sonuç doğuran işlemler için doğrulama kodlarının, işlemi gerçekleştirirken müşterinin onayladığı tutar ve alıcı bilgisine göre spesifik olması, tutar veya fonun aktarılacağı alıcı bilgisindeki herhangi bir değişiklik halinde bu bilgilere göre oluşturulmuş ilgili doğrulama kodunun da geçersiz hale gelmesi temin edilir.*** *Kurumsal internet bankacılığı müşterileri için yığın halinde birden fazla alıcı için toplu işlem gerçekleştirilmesine izin verilen fon transferi gibi işlemlerde, üretilecek doğrulama kodunun ilgili yığın işlem toplam tutarı ve alıcılar için spesifik olması gerekir. Müşteriye atanmış bir şifreleme gizli anahtarı ile doğrulama kodunun imzalanmasının mümkün olmadığı hallerde, 34 üncü maddenin yedinci fıkrası saklı kalmak kaydıyla, SMS yoluyla müşteriye doğrulama kodu iletilebilir.*

(1) Mobil bankacılık uygulamasına tanımlanan ***uygulama PIN'inin müşteriye özgü bir şifreleme anahtarına erişmek üzere kullanılması ve bu şifreleme anahtarı yoluyla müşteriyle ilintili eşsiz bir bilginin <u>banka nezdinde çevrimiçi olarak doğrulanması</u>*** **halinde***, 34 üncü maddenin birinci fıkrasında belirtilen iki bileşenli kimlik doğrulama yerine getirilmiş kabul edilir. Benzer şekilde, müşteriye ait bir biyometrik kimlik doğrulama bileşeninin mobil bankacılık uygulamasında kullanılarak müşteriye özgü bir şifreleme anahtarına erişilmesi suretiyle bu şifreleme anahtarı yoluyla müşteriyle ilintili eşsiz bir bilginin banka nezdinde çevrimiçi olarak doğrulanması halinde, 34 üncü maddenin birinci fıkrasında belirtilen iki bileşenli kimlik doğrulama yerine getirilmiş kabul edilir.*

Bu hükümler çerçevesinde, müşteriye atanmış ve özgülenmiş bir şifreleme gizli anahtarının kullanım alanları:

1. Kimlik doğrulama,
2. Yetkilendirme (işlem doğrulama)

işlemlerinden oluşmakta olup, hem internet bankacılığı dağıtım kanalı hem de bu dağıtım kanalının özelleşmiş bir hali olan mobil bankacılık dağıtım kanalında kimlik doğrulama ve yetkilendirme işlemlerinin gerçekleştirilebilmesi için "doğrulama kodu" üretilmesi ve bunun

müşteriye özgü şifreleme gizli anahtarı ile imzalanması şart koşulmuştur.

Diğer taraftan, BSEBY'nin 38 inci maddesinin birinci fıkrası ile 39 uncu maddesinin ikinci fıkrası aşağıdaki hükümleri amirdir:

(1) İnternet bankacılığı dağıtım kanalında 34 üncü maddenin birinci fıkrasına göre gerçekleştirilecek kimlik doğrulama işleminin ***çevrimdışı olarak lokalde değil banka nezdinde çevrimiçi gerçekleşmesi ve müşterinin bildiği unsurun****, mobil bankacılık uygulaması ya da internet tarayıcısı tarafından hatırlanarak veya bu unsurun başka lokal kimlik doğrulama yöntemlerine bağlanarak otomatik olarak gönderilmemesi gerekir.* ***Müşterinin bildiği unsurun*** *müşteri tarafından girilmesi zorunlu tutulur ve 34 üncü maddenin ikinci fıkrası hükmü saklı kalmak kaydıyla bu unsur* ***lokalde değil banka nezdinde çevrimiçi doğrulanır****.*

(2) ***Mobil bankacılık uygulaması kontrolünde olmayıp cihaz üreticisi kontrolünde olan parola, PIN ya da biyometrik veriler, 34 üncü maddenin birinci fıkrasında belirtilen müşterinin bildiği ya da biyometrik karakteristiği olan unsurlar olarak kullanılamaz.***

BSEBY'nin 38 ve 39 uncu maddelerinin bu hükümleri birlikte değerlendirildiğinde, şifreleme gizli anahtarının içerik imzalama öncesi aktifleştirilmesi için kullanılacak **"PIN" gibi "müşterinin bildiği unsurun" mobil uygulamanın yüklü olduğu cihaz üzerinde lokalde değil, banka nezdinde çevrimiçi doğrulanması gerekmektedir.**

Bu itibarla, bankanın kimlik doğrulamada ve işlem imzalamada müşterilerine kullandıracağı unsurları, işbu Genelge ekinde yer verilen açıklamalara uygun olarak kullandırması halinde, BSEBY'nin 34 üncü maddesinin onbeşinci fıkrasında yer verilen:

(15) Banka, akıllı telefonlar gibi birden fazla kimlik doğrulama bileşeninin bankaya iletilmesinde kullanılan mobil cihazlar üzerindeki bankacılık uygulamalarının kullandığı hassas verilerin, aynı mobil cihaz üzerindeki diğer uygulamalar ve çalışmakta olan işlemler tarafından erişilemez olmasını sağlayacak önlemler alır. Banka, söz konusu mobil cihazların kaybolması ya da çalınması halinde bunlar üzerindeki hassas verilerin yetkisiz kişilerce erişilemez olmasını sağlamak ve mobil cihazların ele geçirilmesi, güvenilirliğinin bozulması, işletim sistemi yazılımının kırılması veya değiştirilmesi gibi hallerden kaynaklanacak risklerin azaltılması amacıyla günün teknolojisine uygun kontroller tesis etmekle yükümlüdür.

hükmün şartları da yerine getirilmiş sayılacaktır.

Ayrıca, BSEBY'nin 34 üncü maddesinin yedinci fıkrası ve 38 inci maddenin üçüncü fıkrası uyarınca, mobil bankacılık uygulamasının ilk kurulumu, aktifleştirilmesi, yeniden aktifleştirilmesi ya da uygulamanın kullanılamaz olması durumları haricinde, mobil bankacılık uygulamasını yükleyerek aktifleştirmiş olan müşterilere, oturum açma ya da oturumun devamında herhangi bir işlemin doğrulanması için hiçbir şekilde SMS ile OTP ya da "doğrulama kodu" gönderilmesi mümkün bulunmamakta olup, SMS ile yapılacak bu tür bildirimlere, yalnızca bu hükümlerde belirtilen istisnai durumlarda başvurulması ve bunun rutin bir uygulama haline getirilmemesi gerekmemektedir. Çünkü SMS ile

gönderilen OTP ya da doğrulama kodunun, aynı mobil cihaz üzerinde yüklü diğer uygulamalar tarafından okunmayacağı ve bu uygulamalar tarafından üçüncü bir tarafa (örn. bir saldırgana) yönlendirilmeyeceğinin garantisi bulunmadığı gibi mobil cihaz üzerindeki "SMS mesajlaşma uygulaması" bankanın kendi kontrolünde olan bir mobil uygulama niteliğinde de bulunmadığı için müşteriye SMS ile gösterilecek OTP ya da doğrulama kodunun bütünlüğü ya da güvenilirliği konusunda da yeterli güvence sağlanamayabileceği tabiidir.

2. Müşteri Onayına Hangi Bilgiler Sunulmuş ise O Bilgilere Göre İşlem İmzalamanın/Onayının Gerçekleştirilmesinin Sağlanması Prensibi *(BSEBY Madde 35-38 / UKTY Madde 12):*

BSEBY'nin "inkâr edilemezlik ve sorumluluk atama" başlıklı 35 inci maddesine göre bankaların, sunmakta oldukları elektronik bankacılık hizmetleri kapsamında gerçekleştirilen işlemlerde hem kendileri hem de müşterileri için **inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikler kullanmaları** gerekmektedir.

BSEBY'nin 38 inci maddesinin üçüncü fıkrasına göre ise finansal sonuç doğuran işlemler için **doğrulama kodlarının, işlemi gerçekleştirirken müşterinin onayladığı tutar ve alıcı bilgisine göre spesifik olması, tutar veya fonun aktarılacağı alıcı bilgisindeki herhangi bir değişiklik halinde bu bilgilere göre oluşturulmuş ilgili doğrulama kodunun da geçersiz hale gelmesi gerekmekte ve doğrulama kodlarının müşteriye atanmış bir şifreleme gizli anahtarı ile imzalanmış şekilde tek kullanımlık olarak üretilmesi gerekmektedir.**

BSEBY'nin 38 inci maddesinin dördüncü fıkrası uyarınca da "*müşterinin gerçekleştirdiği finansal sonuç doğuran işlemler için doğrulama kodunun oluşturulması, iletilmesi ve kullanılması da dâhil olmak üzere doğrulama sürecinin her aşamasında, tutar ve alıcı bilgisi gibi* ***müşteriye gösterilen ve onayına sunulan bilgilerin gizliliğini, güvenilirliğini ve bütünlüğünü sağlamaya yönelik ve internet bankacılığı oturumu esnasındaki veri iletişiminin yetkisiz kişilere yönlendirilmesi riskine karşı gerekli önlemlerin alınması****"* şart koşulmuştur. Bu sebepten işlem doğrulama kodunun müşteriye özgülenmiş şifreleme gizli anahtarı ile güvenli bir şekilde imzalanması ve bu imzalanmış içeriğin banka nezdinde gizlilik ve bütünlük kontrollerinin yerine getirilmesi bakımından doğrulamadan geçirilmesi elzemdir.

Bu itibarla, şifreleme gizli anahtarlarının müşterilere dağıtım süreci ve müşterilerin bu anahtarları nasıl aktive ederek içerik imzaladıkları da bir o kadar önem arz etmektedir. BSEBY'nin 34 üncü maddesinin dördüncü ve beşinci fıkralarında yer verilen aşağıdaki hükümler bu hususun altını çizmektedir:

(4) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasında kullanılacak bileşenlerin üretim aşamalarından başlayarak kullanıcıya ulaştırılmasına kadar geçen sürecin tamamı boyunca güvenliği sağlanır.

(5) Kimlik doğrulamada kullanılacak şifreleme anahtarları; bu anahtarların ele geçirilme ihtimallerini en aza indiren, gizliliğini sağlayan, değiştirilmesini ve bozulmasını önleyen yöntemler barındıracak şekilde müşteri kullanımına sunulur.

BSEBY'nin söz konusu hükümlerinden de anlaşılacağı üzere, müşterinin kendisine atanmış bir şifreleme gizli anahtarı ile doğrulama kodlarının imzalanması sağlansa bile BSEBY aynı zamanda bu imzalama işlemlerinin inkar edilemezlik ve sorumluluk atamayı mümkün kılacak teknikleri barındırmasını beklemekte, diğer bir değişle hem müşteriye atanan şifreleme gizli anahtarının güvenli bir şekilde müşteriye atanması ve müşteriye özgülenmiş olması sağlanarak yetkisiz kişilerce kullanılmasını engelleyecek önlemlerin tesis edilmesi, hem de müşteriye imzalatılan içeriğin gerçekten müşterinin görüp onayladığı içerik olmasının sağlanması gerekmektedir.

UKTY'nin 12 nci maddesinin ikinci fıkrasında ise BSEBY'nin 38 ve 39 uncu maddelerine atıfta bulunulmak suretiyle aşağıdaki hükümlere yer verilmiştir:

"(2) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılmasını ya da şubeler aracılığıyla müşteri kimliğinin yüz yüze tespit edilmesini müteakiben, ***mesafeli olsun olmasın, müşterilerce gerçekleştirilmek istenen işlemlere yönelik olarak bir bilişim veya haberleşme cihazı üzerinden yazılı şeklin yerine geçecek nitelikte bir sözleşme ilişkisi kurulabilmesi için****;*

a) ***Söz konusu sözleşmenin bütün şartlarının, müşterinin okuyabileceği şekilde internet bankacılığı ya da mobil bankacılık dağıtım kanalları üzerinden müşteriye iletilmesi****,*

b) (a) bendine göre müşteriye iletilen sözleşme ve bu sözleşme ile birlikte müşterinin ***sözleşmeyi kuran irade beyanının, BSEBY'nin 38 inci maddesinin üçüncü fıkrası ile 39 uncu maddesinin birinci fıkrasında belirtilen müşteriye özgü şifreleme gizli anahtarı ile imzalanarak bankaya iletilmesi****,*

c) ***(a) bendine göre iletilen sözleşmede müşteriye sözleşme içeriği olarak hangi bilgiler gösterilmiş ise (b) bendine göre müşteri tarafından yalnızca o bilgilerin imzalanmasının sağlanması****,*

şarttır."

Söz konusu hükümler, özünde müşteri onayına hangi bilgiler sunulmuş ise o bilgilere göre işlem imzalamanın/onayının gerçekleştirilmesinin sağlanması prensibini **(WYSIWYS)** ifade etmekte olup, gerek doğrulama kodlarının kullanılması suretiyle kimlik doğrulama ve işlem doğrulama işlemlerinin gerçekleştirilmesi, gerekse bir bilişim veya haberleşme cihazı üzerinden yazılı şeklin yerine geçecek nitelikte bir sözleşme ilişkisi kurulabilmesi için müşteriye özgü şifreleme gizli anahtarları ile gerçekleştirilecek imzalama işleminin bu hükümlere ve bu prensibe uygun olması gerekmektedir.

Bu itibarla, söz konusu imzalama işlemlerinin yukarıda anılan hükümlere ve WYSIWYS prensibine uygunluğunun sağlanabilmesi için kullanılacak metodolojinin aşağıdaki açıklamalara uygun olması gerekmektedir:

1. Öncelikle bankanın işlem imzalamada kullanılmak üzere, mobil uygulaması içinde bu işlemlere özgü güvenli bir ortam yaratmak ve BSEBY'nin 34 üncü maddesinin onbeşinci fıkrasından kaynaklanan yükümlülüklerini yerine getirmek üzere
    i. Spesifik bir Yazılım Geliştirme Kiti (SDK) ve
    ii. Doğrudan bu SDK ile güvenli ayrı bir kanaldan iletişim kuracak şekilde yapılandırılmış bir Güvenlik Sunucusu (SS)

   oluşturması gerekmektedir.

2. İşlem imzalamada kullanılacak müşteriye özgü şifreleme gizli anahtarının, SDK kontrolündeki güvenli bir alanda şifrelenmiş bir şekilde saklanması ve yalnızca SS'nin gerçekleştireceği güvenlik kontrolleri sonrası ve yalnızca SS tarafından sunulacak anahtar ile şifresinin çözülmesi diğer bir deyişle işlem imzalama için aktifleştirilmesi gerekmektedir.

3. SS'nin şifreleme gizli anahtarını aktifleştirmesi için, imzalama talebinin gerçekten "müşterinin sahip olduğu" kimlik doğrulama unsuru niteliğinde olan bankanın güvenli mobil uygulamasından geldiğini teyit edecek güvenlik kontrollerini gerçekleştirmesi gerekmekte ve bu güvenlik kontrolleri için SS'ye sağlanacak risk verileri SDK'nin arkada planda sürekli bir şekilde çalışan güvenlik sensörleri yoluyla SDK ile SS arasındaki tahsisli güvenli ayrı bir kanaldan (Out-of-Band) SS'ye iletilmelidir.

4. SDK'nin güvenlik sensörleri, BSEBY'nin 34 üncü maddesinin onbeşinci fıkrasına uygun olacak şekilde, sürekli bir biçimde asgari olarak aşağıdaki kontrolleri sağlayarak SS'ye iletilmek üzere gerekli risk verilerini oluşturmalıdır:
    i. Mobil uygulama güvenilirliğinin bozulmasına ilişkin kontroller,
        a) Hassas verilerin kullanıcı arayüzü üzerinden girilmesi esnasında çalınmasını engellemeye yönelik kontroller (**anti-keylogging**)
        b) Çalışmakta olan SDK kodunun çalışma anında değiştirilmediğine ve araya zararlı kod parçalarının eklenmediğine ilişkin kontroller (**anti-injection**)
        c) Aktive edilmiş mobil bankacılık uygulaması ve SDK'nin yalnızca aktivasyon sırasında kaydedilmiş mobil cihaz üzerinde çalıştığına ilişkin kontroller (**device-binding**)
    ii. Mobil cihaz güvenilirliğinin bozulmasına ilişkin kontroller,
        a) Mobil cihazın zararlı yazılım barındırıp barındırmadığı ya da bu yazılımlarca ele geçirilip geçirilmediğine ilişkin kontroller (**anti-malware**),
        b) Mobil cihaz işletim sisteminin kırılıp kırılmadığına (**jailbreaking**) ilişkin kontroller,

5. SS ile SDK arasındaki kanalın güvenliğinin sağlanabilmesi için, mobil bankacılık uygulaması ve SDK'nin ilk aktivasyonu sırasında, henüz aktive edilmemiş SDK örneğinde(instance) önyüklü olarak bulunması gereken SS'nin sunucu sertifikası

yoluyla güvenli bir TLS bağlantısı kurulması sağlanmalı ve sonrasında aktivasyonu gerçekleşen SDK örneği ve mobil cihaza özgü olacak şekilde SS tarafından üretilen istemci sertifikasının bu güvenli bağlantı üzerinden ilgili SDK örneğine atanması suretiyle, söz konusu istemci-sunucu sertifikaları üzerinden SS ve SDK arasındaki iletişimde kullanılacak uçtan uca güvenli bağlantı kanalının kurulması sağlanmalıdır.

6. Her bir SDK örneğinin(instance), ancak 4.maddede belirtilen güvenlik sensörleri üzerinden oluşturduğu risk verileri üzerinden SS'nin bütünlük kontrolünden geçmek ve SS'nin kendisine atadığı istemci sertifikası yoluyla kimliğini SS'ye doğrulamak kaydıyla, müşterinin girdiği PIN/bilinen unsur için doğrulama isteği gönderebilmesi sağlanmalı ve 3.madde de belirtildiği üzere SDK ile SS arasındaki iletişim, mobil bankacılık uygulaması ile banka arkayüzü (back-end) arasındaki iletişim kanalından ayrı ve yalnızca SS ve SDK arasındaki iletişime tahsisli uçtan uca güvenli ayrı bir kanal (Out-of-Band) üzerinden yapılmalıdır.

7. Mobil bankacılık uygulaması ve SDK'nın ilk aktivasyonu sırasında,
    i. Müşterinin "bildiği unsur" olarak kullanacağı PIN ya da parolanın, SDK tarafından salted-hash (tuzlanmış kriptografik özet) haline dönüştürülerek SS veritabanında saklanmak üzere SS'ye gönderilmesi;
    ii. SS'nin aynı zamanda bir "Sertifika Otoritesi" rolü oynayarak, aktivasyonu gerçekleşen SDK örneği ve mobil cihaza özgü olacak şekilde RSA algoritmasına göre oluşturulmuş en az 2048 bit uzunluğunda bir asimetrik şifreleme anahtar çifti oluşturması ve anahtar çiftlerinden gizli olanını yalnızca SS'de tutulan bir simetrik şifreleme anahtarı ile şifreleyerek SDK'nin kontrolündeki güvenli bir alanda bu simetrik anahtarla şifrelenmiş olarak saklanmak üzere SDK'ye iletmesi

   gerekmektedir.

8. 7.maddede belirtilen PIN/bilinen unsura ilişkin salted-hash verisi SDK tarafında hiçbir şekilde saklanmamalı ve doğrulama isteğinin gönderilmesini müteakip derhal SDK tarafında silinmeli ve SS veritabanında da PIN/bilinen unsur verisi hiçbir şekilde açık bir şekilde (plain text) saklanmamalı, söz konusu veritabanında bunlara ilişkin salted-hash bilgisi yalnızca şifrelenmiş bir şekilde tutulmalıdır.

9. SDK'nın SS'ye göndereceği PIN/bilinen unsur için doğrulama isteği, işbu Genelge ekinde yer verilen açıklamaların 1.bölümünde de belirtildiği üzere ve BSEBY'nin 11 inci maddesinin üçüncü fıkrasına uygun olarak, müşterinin girdiği PIN/bilinen unsurun salted-hash halinin SS veritabanında bulunan salted-hash hali ile karşılaştırılması yoluyla çevrimiçi doğrulanmalıdır.

10. Müşterinin PIN/bilinen unsur doğrulama işleminin 9.maddede belirtildiği şekilde başarıyla gerçekleşmesi halinde,
    i. SS ve SDK arasındaki tahsisli güvenli kanal üzerinden SS'nin, SDK kontrolündeki güvenli alanda şifrelenmiş bir şekilde tutulan müşteriye özgü

şifreleme gizli anahtarının şifresini çözecek simetrik şifreleme anahtarını SDK'ye iletmesi ve

ii. SDK tarafından bu anahtarla müşteriye özgü şifreleme gizli anahtarının şifresinin çözülmesi suretiyle söz konusu şifreleme gizli anahtarının imzalanacak işlem için aktifleştirilmesi

sağlanmalıdır.

11. SS üzerinden aktifleştirilen şifreleme gizli anahtarı yoluyla,
    i. SDK tarafından üretilen kimlik doğrulamaya yönelik doğrulama kodunun,
    ii. SDK tarafından müşteriye gösterilen bilgiler üzerinden müşterinin onayladığı tutar ve alıcı bilgisine göre spesifik olacak şekilde, SDK tarafından finansal sonuç doğuran işlemler için üretilen doğrulama kodunun,
    iii. SDK tarafından müşteriye gösterilen bilgiler üzerinden müşterinin onayını ve irade beyanını yansıtan elektronik ortamda kurulacak sözleşmelerin

müşteri tarafından elektronik imzalı olarak imzalanması sağlanmalıdır.

3. Arayüz Sağlayıcının Mobil Uygulaması ya da İnternet Tarayıcısı Temelli Arayüzünün, Kimlik Doğrulama ve İşlem Güvenliği Yükümlülüklerine Uygun Olmasının Sağlanması *(DBY Madde 13):*

Bilindiği üzere, DBY'nin 13 üncü maddesinin dördüncü ve beşinci fıkralarında aşağıdaki hükümlere yer verilmiştir:

(4) Servis bankasının arayüz sağlayıcının müşterisine bankacılık hizmetleri sunabilmesi için söz konusu müşteri ile servis bankası arasında Kanunun 76 ncı maddesi uyarınca sözleşme ilişkisinin kurulması gereklidir. ***Söz konusu sözleşme ilişkisinin elektronik ortamda kurulması halinde, sürecin UKTY'ye uygun olarak yürütülmesi ve müşteri kimliğinin UKTY'ye uygun olarak servis bankası tarafından tespit edilmesi zorunludur. Servis bankası ile müşteri arasındaki sözleşme ilişkisi kurulması sürecinin arayüz sağlayıcının mobil uygulaması ya da internet tarayıcısı temelli arayüzü üzerinden başlatılıp yine bu hizmet kanalları üzerinden tamamlanması halinde, arayüz sağlayıcının söz konusu hizmet kanallarının BSEBY'de yer verilen güvenlik kriterlerine uygun olması ve müşteriye sözleşme içeriği olarak hangi bilgiler gösterilmiş ise müşteri tarafından yalnızca o bilgilerin onaylanmasının sağlanması konusunda güvence sağlayacak nitelikte olması servis bankasının sorumluluğundadır.***

(5) Müşterinin servis bankasının sunduğu hizmetlere erişmede kullandığı ***arayüz sağlayıcının mobil uygulaması ya da internet tarayıcısı temelli arayüzünün, BSEBY'nin üçüncü kısmında elektronik bankacılık hizmetlerine ilişkin yer verilen kimlik doğrulama ve işlem güvenliği yükümlülüklerine uygun olmasını sağlamak konusunda arayüz sağlayıcı ve servis bankası müteselsilen sorumludurlar.*** *Servis bankası, bu yükümlülükleri yerine getirmeyen ya da*

sistemleri bu yükümlülükleri yerine getirme konusunda yetersiz olan arayüz sağlayıcılara servis modeli bankacılığı hizmeti sunamaz ve bunlardan destek hizmeti alamaz.

Bu kapsamda, arayüz sağlayacıların mobil uygulaması ya da internet tarayıcısı temelli arayüzünün, BSEBY'nin üçüncü kısmında yer verilen kimlik doğrulama ve işlem güvenliği yükümlülüklerine uygun olmasının gerekmesinin yanı sıra, arayüz sağlayıcıların mobil uygulaması temelli arayüzü üzerinden servis bankası müşterisinin gerçekleştireceği kimlik doğrulamanın ve işlem imzalamanın işbu Genelge ekinin 1. ve 2. bölümlerinde yer verilen açıklamalara uygun olması gerekmektedir.

Bu itibarla, DBY uyarınca arayüz sağlayıcılığı faaliyetinde bulunacakların mobil uygulama arayüzü içinde, servis bankasının SDK'sının gömülü olması ve işbu Genelge ekinin 2.bölümünde belirtilen işlem imzalama akışlarının; bu mobil uygulama arayüzüne gömülü servis bankası SDK'sı ve bu SDK ile tahsisli uçtan uca güvenli ayrı bir kanaldan iletişim kuracak şekilde yapılandırılmış olan servis bankası Güvenlik Sunucusu(SS) üzerinden yürütülmesi gerekmektedir.

4. Kimlik Doğrulama ve İşlem İmzalama Amacıyla Kullanılan, Geliştirilen ve Satın Alınan Ürünlerin İşbu Genelge Ekinde Yer Verilen Açıklamalara İntibakı*:*

Kimlik doğrulama ve işlem imzalama amacıyla kullanılan, kurum içi geliştirilen ya da satın alınan ürünlerin işbu Genelge ekinde yer verilen açıklamalara uygunluğunun sağlanması zorunludur.

Kurum içi geliştirilen ya da satın alınan ürünlerin bu uygunluğu sağladığı, 31.12.2021 tarihli ve 31706 sayılı 6.Mükerrer Resmi Gazete'de yayımlanan Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik uyarınca **gerçekleştirilecek bilgi sistemleri denetimi kapsamında ele alınmak zorundadır.**

Bankalara, Bankacılık Düzenleme ve Denetleme Kurumunun(Kurum) gözetimi ve denetimi altındaki diğer kuruluşlara ve DBY kapsamındaki arayüz sağlayıcılara kimlik doğrulama ve işlem imzalamada kullanılmak üzere ürün satan ya da dış hizmet sağlayan kuruluşlar ise, **Kurumumuza başvurarak,** bu alanda (kimlik doğrulama ve işlem imzalama) bankalara, Kurum gözetimi ve denetimi altındaki diğer kuruluşlara ve arayüz sağlayıcılara ürün ve hizmet sunabilmek için **Kurumdan izin almakla** yükümlüdürler.