T.C.
BANKACILIK DÜZENLEME VE DENETLEME KURUMU

Sayı: 77574904-010.06.02
Konu: Elektronik Bankacılık Hizmetlerinde ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasında Kimlik Doğrulama ve İşlem Güvenliği için Sağlanması Gereken Kriterler Hk.

GENELGE
(2023/1)

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 üncü ve 35 inci maddelerinde elektronik bankacılık hizmet kanallarında kimlik doğrulama ve işlem güvenliğinin nasıl gerçekleştirilmesi gerektiği ve bu kanallar üzerinden gerçekleştirilecek işlemlerde 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 Resmi Gazete'de yayımlanan Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmeliğin (UKTY) 12 nci maddesinin ikinci fıkrasında ise BSEBY'nin 38 inci 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."

Benzer şekilde, 11/01/2022 tarihli ve 31716 sayılı Resmi Gazete'de yayımlanan Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketlerince Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmeliğin (UKTY-2) 12 nci ve 13 üncü maddelerinde de aşağıdaki hükümlere yer verilmiştir:

Kimlik doğrulama ve işlem güvenliği

MADDE 12 – *(1) Bu Yönetmelikte aksi belirtilmedikçe, müşteri bilgilerinin görüntülenmesi gibi finansal sonuç veya yükümlülük doğurmayan işlemler hariç olmak üzere elektronik ortamda sunulan hizmetler için şirketin müşterilerine birbirinden bağımsız en az iki bileşenden oluşan bir kimlik doğrulama mekanizması uygulaması ve bu bileşenlerin kimlik doğrulama sürecinde kullanılmaları esnasında barındırdıkları kimlik doğrulama verilerinin gizliliğini sağlayacak önlemleri alması esastır. Bu iki bileşen; müşterinin "bildiği", "sahip olduğu" veya "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Bileşenlerin bağımsız olması, bir bileşenin ele geçirilmesinin diğer bileşenin güvenliğini tehlikeye atmamasını ifade eder. Müşterinin sahip olduğu bileşenin müşteriye özgü olması ve taklit edilememesi esastır.*

...

(13) ***Elektronik ortamda sunulan hizmetlerde birinci fıkraya göre gerçekleştirilecek kimlik doğrulama işlemi için müşteriye atanmış bir şifreleme gizli anahtarı ile imzalanacak şekilde tek kullanımlık bir doğrulama kodu üretilir.*** *Doğrulama kodu aracılığıyla birinci fıkrada belirtilen kimlik doğrulama unsurlarından hiçbiri hakkında bilgi edinilememesi, bilinen bir doğrulama kodu ile geçerli başka doğrulama kodlarının türetilememesi, doğrulama kodlarının taklit edilememesi sağlanır. Müşteriye atanmış bir şifreleme gizli anahtarı ile doğrulama kodunun imzalanmasının mümkün olmadığı hallerde, yedinci fıkra hükmü saklı kalmak kaydıyla SMS yoluyla müşteriye doğrulama kodu iletilebilir.*

(14) Elektronik ortamda sunulan hizmetin mobil uygulama vasıtasıyla verilmesi durumunda, uygulama PIN'inin veya müşteriye ait bir biyometrik kimlik doğrulama bileşeninin müşteriye özgü bir şifreleme anahtarına erişmek üzere kullanılması ve bu şifreleme anahtarı yoluyla müşteriyle ilintili eşsiz bir bilginin şirket nezdinde çevrimiçi olarak doğrulanması halinde, birinci fıkrada belirtilen iki bileşenli kimlik doğrulama yerine getirilmiş kabul edilir.

Kimlik tespitini müteakip sözleşme ilişkisinin kurulması

MADDE 13 – *(1) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılmasını ya da müşteri kimliğinin yüz yüze tespit edilmesini müteakiben, müşterilerce gerçekleştirilmek istenen işlemlere yönelik* ***sözleşme ilişkisinin internet veya mobil hizmet kanalları üzerinden mesafeli olarak kurulması durumunda, müşterinin sözleşmeyi kuran irade beyanının aynı kanallar üzerinden 12 nci maddenin birinci fıkrasına uygun olarak gerçekleştirilmiş bir kimlik doğrulama sonrasında alınması şarttır.***

(2) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılmasını ya da 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 veya mobil hizmet kanalları üzerinden müşteriye iletilmesi,***

b) (a) bendine göre müşteriye iletilen sözleşme ve bu sözleşme ile birlikte müşterinin ***sözleşmeyi kuran irade beyanının, 12 nci maddenin on üçüncü fıkrası ile on dördüncü fıkrasında belirtilen müşteriye özgü şifreleme gizli anahtarı ile imzalanarak şirkete 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 ve 93 üncü maddesi ile 6361 sayılı Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanununun 15 inci, 22 nci, 38 inci, 39 uncu ve 39/A maddeleri çerçevesinde alınan 23.03.2023 tarihli ve 10546 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] [2]

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*

---

[1] İşbu Genelge ekindeki açıklamalarda yer verilen "banka" ifadelerinin 6361'e tabi kuruluşlar için ilgili kuruluşları(Şirketleri) ifade ettiği kabul edilir ve "internet bankacılığı" ya da "mobil bankacılık" dağıtım kanalları;

i. 6361 sayılı Kanuna tabi kuruluşlar ile Kurumun gözetim ve denetimine tabi banka dışındaki diğer kuruluşlar için, söz konusu kuruluşların müşterilerine internet ya da mobil cihazlar üzerinden hizmet sunduğu dağıtım kanalları olarak;

ii. 6361 sayılı Kanunun 8 inci maddesinin birinci fıkrası uyarınca, şube dışında teşkilatlanma ve acentelik verme yasağının istisnası olarak işlem gerçekleştirilmesine izin verilmiş olan Kurulca belirlenen bilgi sistemleri ya da platformlar için, söz konusu bilgi sistemlerinin/platformların müşterilerine internet ya da mobil cihazlar üzerinden hizmet sunduğu dağıtım kanalları olarak

ele alınır.

[2] 6361 sayılı Kanunun 39 uncu maddesinin ikinci fıkrası uyarınca finansman şirketlerinin, kredilendirecekleri mal veya hizmetleri temin eden satıcılarla uzaktan iletişim araçlarının kullanılması suretiyle mesafeli olarak genel bir sözleşme ilişkisi kurabilmesi için, söz konusu gerçek ya da tüzel kişi tacir niteliğindeki satıcıların finansman şirketlerinin müşterisi olarak ele alınması; satıcı statüsündeki bu müşterilerin Kurumun gerçek ya da tüzel kişi müşterilerin uzaktan kimlik tespitinin yapılmasına ilişkin düzenlemelerine uygun olarak kimlik tespitlerinin yapılması ve satıcı statüsündeki bu müşteriler ile işbu Genelge ekindeki açıklamalara uygun olarak elektronik ortamda sözleşme ilişkisinin kurulması sağlamalıdır.

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 inci ve 39 uncu maddelerinin bu hükümleri birlikte değerlendirildiğinde, içerik imzalama öncesi şifreleme gizli anahtarına erişmek 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 on beşinci 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 anahtarlara nasıl erişerek 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 maddesinde ise BSEBY'nin 34 üncü, 38 inci ve 39 uncu maddelerine atıfta bulunulmak suretiyle aşağıdaki hükümlere yer verilmiştir:

"(1) Bu Yönetmelikte yer alan şartlar dâhilinde uzaktan kimlik tespitinin yapılmasını ya da şubeler aracılığıyla müşteri kimliğinin yüz yüze tespit edilmesini müteakiben, BSEBY'de düzenlenen internet bankacılığı ya da mobil bankacılık dağıtım kanallarından herhangi biri kullanıma açık olan müşterilerce gerçekleştirilmek istenen işlemlere yönelik sözleşme ilişkisinin mesafeli olarak kurulması durumunda, müşterinin sözleşmeyi kuran irade beyanının ***BSEBY'nin 34 üncü maddesinin birinci fıkrasına uygun olarak gerçekleştirilmiş bir kimlik doğrulama sonrasında*** *söz konusu dağıtım kanalları üzerinden alınması şarttır.*

(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."

UKTY-2'nin 12 nci ve 13 üncü maddelerinde de aynı hususları amaçlayan benzer hükümlere yer verilmiş olup, söz konusu tüm bu hükümler, özünde müşteri onayına hangi bilgiler sunulmuş ise o bilgilere göre işlem imzalamanın/onayının gerçekleştirilmesinin sağlanması prensibini (**WYSIWYS)** ifade etmektedir. Dolayısıyla, gerek doğrulama kodlarının kullanılması suretiyle kimlik doğrulama ve işlem doğrulamanın gerçekleştirilmesi, gerekse internet bankacılığı ya da mobil bankacılık dağıtım kanallarından herhangi biri kullanıma açık olan müşteriler ile sözleşme ilişkisinin mesafeli olarak kurulabilmesi için veya müşteriler ile 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 on beşinci 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 anahtarı ile buna karşılık gelen açık anahtarın(asimetrik anahtar çiftinin), müşterinin mobil bankacılık uygulamasının yüklü olduğu mobil cihazında bulunan ve asimetrik anahtar çifti oluşturabilen ve oluşturulan anahtar çiftlerinden şifreleme gizli anahtarını kopyalanmaya ve dışarıya çıkarılmaya imkan vermeyecek şekilde saklayabilen (iOS cihazlar için "Secure Enclave", Andorid cihazlar için "hardware backed keystore" ya da "Strong Box" gibi) kriptografik donanım biriminde SDK tarafından oluşturulması ve SDK tarafından müşteriye özgü olarak oluşturulan şifreleme gizli anahtarının bu donanım birimlerinde saklanması ve imzalama işlemi için yalnızca SDK tarafından kullanılabiliyor olması gerekmektedir. Şifreleme gizli anahtarının "müşteriye özgü" olması, müşteriye bağlanmış (binded) mobil cihaza ve o cihaz üzerindeki aktifleştirilmiş SDK örneğine (instance) özgülenmiş bir gizli anahtar olmasını ifade

eder. Asimetrik anahtar çifti oluşturmada kullanılacak algoritmaların ve anahtar uzunluklarının, BSEBY'nin 9 uncu maddesinin ikinci fıkrası çerçevesinde günün teknolojine uygun olarak seçilmesi zorunludur.

3. SDK tarafından müşteri mobil cihazı üzerindeki kriptografik donanım birimine ürettirilen ve yalnızca SDK tarafından imzalama işleminde kullanılabilen müşteriye özgü şifreleme gizli anahtarı için gelecek "imzala işlemi taleplerinin" yalnızca SS'nin gerçekleştireceği güvenlik kontrolleri sonrası ve yalnızca 2. maddede belirtilen asimetrik anahtar çiftlerinden müşteriye özgü şifreleme gizli anahtarının diğer çifti olan müşteriye özgü açık anahtar ile şifrelenmiş bir şekilde müşteri için aktifleştirilmiş SDK örneğine SS tarafından gönderilmesi sağlanmalıdır.

4. SS'nin ilgili SDK örneğine imzalama talebinde bulunabilmesi için, ilgili SDK örneğinin arka planda sürekli bir şekilde çalışan güvenlik sensörleri yoluyla güvenli mobil uygulama ve güvenli mobil cihaz üzerinde çalıştığını teyit edecek güvenlik kontrollerini gerçekleştirmesi gerekmekte ve bu güvenlik sensörlerinden sağlanacak risk verileri SDK ile SS arasındaki tahsisli güvenli ayrı bir kanaldan (Out-of-Band) SS'ye iletilmelidir.

5. SDK'nin güvenlik sensörleri, BSEBY'nin 34 üncü maddesinin on beşinci fıkrasına uygun olacak şekilde, sürekli bir biçimde asgari olarak aşağıdaki kontrolleri sağlayarak SS'ye iletilmek üzere gerekli risk verilerini oluşturmalıdır:
    - *i.* Mobil uygulama güvenilirliğinin ve bütünlüğünün 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) Çalışmakta olan SDK kodunun debugger ortamında, emülatör ortamında ya da sanal makinede çalışmakta olup olmadığına ilişkin kontroller (**anti-debugging ve anti-emulation**)
        d) Aktive edilmiş mobil bankacılık uygulaması ve SDK'nin yalnızca aktivasyon sırasında kaydedilmiş mobil cihaz üzerinde çalıştığına ilişkin kontroller (**device-binding**)
    - *ii.* Mobil cihaz güvenilirliğinin ve bütünlüğünün 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,

6. SS ile SDK arasındaki kanalın güvenliğinin sağlanabilmesi için, mobil bankacılık uygulaması ve SDK'nin ilk aktivasyonu sırasında, henüz aktive edilmemiş SDK

örneği ile SS arasında 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 asimetrik anahtar çiftlerinden şifreleme gizli anahtarının bu güvenli bağlantı üzerinden ilgili SDK örneğine iletilmesi ve SDK kontrolündeki güvenli bir alanda şifrelenmiş bir şekilde saklanması sağlanmalıdır. SS tarafından aktivasyonu gerçekleşen SDK örneği için üretilen asimetrik anahtar çiftlerinden "gizli" olanı SS tarafından saklanmamalı ve ilgili SDK örneğine iletilir iletilmez silinmeli, söz konusu anahtar çiftlerinden "açık" olanı ise SS tarafından imzalanarak ilgili SDK örneğine atanmış bir istemci sertifikasına dönüştürülmek suretiyle söz konusu güvenli bağlantı üzerinden ilgili SDK örneğine iletilmelidir. Bu adımlar sonrasında ilgili SDK örneği ile SS arasındaki iletişimde söz konusu sunucu ve istemci sertifikalarının kullanılması yoluyla çift yönlü kurulacak bir mTLS bağlantısı (Mutual TLS) üzerinden uçtan uca güvenli bir iletişim kanalının tesis edilmesi ve bu iletişim kanalının mobil bankacılık uygulaması ile banka arkayüzü (back-end) arasındaki iletişim kanalından ayrı ve yalnızca SS ve SDK arasındaki iletişime tahsisli güvenli ayrı bir kanal (Out-of-Band) olarak yapılandırılması sağlanmalıdır. Asimetrik anahtar çifti oluşturmada kullanılacak algoritmaların ve anahtar uzunluklarının, BSEBY'nin 9 uncu maddesinin ikinci fıkrası çerçevesinde günün teknolojine uygun olarak seçilmesi zorunludur.

7. Her bir SDK örneğinin(instance), ancak 5. maddede belirtilen güvenlik sensörleri üzerinden oluşturduğu risk verileri üzerinden SS'nin güvenilirlik ve bütünlük kontrollerinden geçmiş olması kaydıyla, SS'nin kendisine atadığı istemci sertifikası yoluyla 6. maddede belirtilen şekilde kurulmuş olan uçtan uca güvenli bir iletişim kanalı üzerinden, müşterinin girdiği PIN/bilinen unsuru için SS'e doğrulama isteği gönderebilmesi sağlanmalıdır.

8. Mobil bankacılık uygulaması ve SDK'nın ilk aktivasyonu sırasında,
    i. Müşterinin "bildiği unsur" olarak kullanacağı PIN ya da parolanın, SDK tarafından kriptografik özet (hash) haline dönüştürülerek SS'ye gönderilmesi ve bu kriptografik özetin tuzlanmış özet (salted-hash) haline dönüştürülerek SS veritabanında şifrelenmiş bir şekilde saklanması;
    ii. Aktifleştirilmiş SDK örneğinin 2. madde uyarınca müşteriye özgü asimetrik anahtar çifti oluşturması ve bu anahtarlardan "açık" olanını SS'ye iletmesi,
    iii. SS'nin aynı zamanda bir "Sertifika Otoritesi" rolü oynayarak, aktifleştirilmiş SDK örneği tarafından müşteriye özgü olarak kendisine iletilen açık anahtar için müşteriye özgü bir sertifika üretmesi, müşteri tarafından imzalanan içeriğin teyidi için bu sertifikayı kullanması ve SDK örneğinin kullanım dışı bırakılması gereken durumlarda söz konusu sertifikayı geçersiz hale getirmesi

gerekmektedir.

9. 8. maddede belirtilen PIN/bilinen unsur bilgisi ya da bu unsura ilişkin kriptografik özet (hash) verisi SDK tarafında hiçbir şekilde saklanmamalı ve doğrulama isteğinin gönderilmesini müteakip derhal SDK tarafında silinmeli ve SS veritabanında da PIN/bilinen unsur ya da bu unsura ilişkin kriptografik özet (hash) verisi hiçbir şekilde açık bir şekilde (plain text) saklanmamalı, söz konusu veritabanında SDK tarafından gönderilen hash verisi, tuzlanmış özet (salted-hash) haline dönüştürülerek SS veritabanında yalnızca şifrelenmiş bir şekilde tutulmalıdır.

10. 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 hash halinin SS veritabanında bulunan salted-hash hali ile karşılaştırılması yoluyla çevrimiçi doğrulanmalıdır.

11. Müşterinin PIN/bilinen unsur doğrulama işleminin 10. maddede belirtildiği şekilde başarıyla gerçekleşmesi halinde,
    - *i.* SS ve SDK arasındaki tahsisli güvenli kanal üzerinden SS'nin 3. ve 8. maddede belirtilen müşteriye özgü sertifikadaki açık anahtar ile şifrelenmiş bir şekilde SDK'ye kimlik doğrulamaya yönelik bir "işlem imzalama talep mesajı" (challenge) göndermesi,
    - *ii.* SDK tarafından alınan bu mesajın ise müşteri mobil cihazının kriptografik donanım biriminde bulunan müşteriye özgü şifreleme gizli anahtarı ile açılmak suretiyle, SDK'nın kimlik doğrulamaya yönelik bir "işlem imzalama onay mesajını" (response) aynı anahtarla imzalayarak kimlik doğrulamaya yönelik bir doğrulama kodu oluşturması ve bunu SS'e göndermesi,
    - *iii.* SS'in, SDK'dan kendisine iletilen doğrulama kodunu müşteriye özgü açık anahtar ile açarak doğruluğunu teyit etmesi,
    - *iv.* Teyit edilmiş doğrulama kodu için SS'in banka arkayüzü (back-end) ile arasındaki uçtan uca güvenli iletişim kanalından back-end'e kullanıcıyı içeriye alması (login) yönünde mesaj iletilmesi ve bu mesaj sonrasında back-end'in kullanıcıyı içeriye alması (login) ,
    - *v.* Bu aşamaların tamamlanmasını müteakip ilgili doğrulama kodu için zaman damgası oluşturularak banka log sunucusuna aktarılması

    sağlanmalıdır. Challenge-Response mesajlarının tekrarlama (replay) saldırılarını engellemek üzere tek kullanımlık bir değer (nonce) içermesi zorunludur.

12. Müşteri mobil cihazının kritptografik donanım biriminde bulunan ve yalnızca aktifleştirilmiş SDK örneği tarafından kullanılabilen müşteriye özgü 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.

13. 12. madde çerçevesinde finansal sonuç doğuran işlemler ile elektronik ortamda sözleşme kurulmasına ilişkin (*12.ii ve 12.iii*) SDK tarafından imzalanmak üzere müşteriye içerik gösterilmesi öncesinde, müşterinin başlattığı işlemlerin mobil bankacılık uygulaması tarafından öncelikle back-end sunucusuna iletilmesi ve back-end sunucusunun bu müşteri talebini doğrulanmak üzere uçtan uca güvenli kanaldan SS'e iletmesi gerekmektedir. Back-end'den SS'e müşteri talebinin iletilmesi sonrasında bu talebe ilişkin;

i. SS ve SDK arasındaki tahsisli güvenli kanal üzerinden SS'nin 3. ve 8. maddede belirtilen müşteriye özgü sertifikadaki açık anahtar ile şifrelenmiş bir şekilde SDK'ye "işlem imzalama talep mesajı" (challenge) göndermesi,

ii. SDK tarafından alınan bu mesajın ise müşteri mobil cihazının kritptografik donanım biriminde bulunan müşteriye özgü şifreleme gizli anahtarı ile açılmak suretiyle ve yine SDK tarafından müşteriye gösterilecek şekilde bir onay ekranı çıkarması,

iii. SDK tarafından müşteriye gösterilen onay ekranındaki bilgilerin müşteri tarafından onaylanması halinde, onaylanan bu bilgiler için SDK'nın, müşteriye özgü şifreleme gizli anahtarı ile "işlem imzalama onay mesajını" (response) imzalayarak bir doğrulama kodu oluşturması ve bunu SS'e göndermesi,

iv. SS'in, SDK'dan kendisine iletilen doğrulama kodunu müşteriye özgü açık anahtar ile açarak, back-end'den iletilen bilgiler ile karşılaştırmak suretiyle bu bilgilerin değişmediğine ilişkin bütünlük kontrolünü gerçekleştirmesi ve bilgilerin doğruluğunu teyit etmesi,

v. Teyit edilmiş doğrulama kodu için SS'in banka arkayüzü (back-end) ile arasındaki uçtan uca güvenli iletişim kanalından back-end'e ilgili işlemi gerçekleştirmesi yönünde mesaj iletilmesi ve bu mesaj sonrasında back-end'in kendisi için doğrulama kodu oluşturulmuş işlemi gerçekleştirmesi,

vi. Bu aşamaların tamamlanmasını müteakip ilgili doğrulama kodu için zaman damgası oluşturularak banka log sunucusuna aktarılması

sağlanmalıdır. Challenge-Response mesajlarının tekrarlama (replay) saldırılarını engellemek üzere tek kullanımlık bir değer (nonce) içermesi zorunludur.

14. 10. madde çerçevesinde PIN/bilinen unsurun doğrulaması, 11. madde çerçevesinde de müşterinin sahip olduğu unsur niteliğindeki müşteriye özgü şifreleme gizli anahtarı yoluyla geçerli bir doğrulama kodu oluşturulması sonrasında gerçekleşecek iki bileşenli kimlik doğrulamaya dayalı login işlemini müteakip açılan **kullanıcı oturumunun geçerli olduğu süre boyunca,**

i. 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,

ii. SDK tarafından müşteriye gösterilen bilgiler üzerinden müşterinin onayını ve irade beyanını yansıtan elektronik ortamda kurulacak sözleşmelerin

12. maddeye uygun olarak müşteriye özgü şifreleme gizli anahtarı ile imzalanması sürecinde müşterinin yeniden PIN/bilinen unsur doğrulaması yapması gerekmemektedir. BSEBY'nin 39 uncu maddesinin üçüncü fıkrası uyarınca müşterinin iki bileşenle kimlik doğrulama gerçekleştirerek açtığı son oturumun üzerinden 90 günden daha fazla bir süre geçmemiş olması kaydıyla yalnızca sahip olunan kimlik doğrulama unsuru ile gerçekleştirilebilen işlemler için PIN/bilinen unsur doğrulamasının tekrar yapılması gerekmemekle birlikte, söz konusu fıkra uyarınca gerçekleştirilecek login işlemleri ile finansal sonuç doğuran işlemler için müşteriye özgü şifreleme gizli anahtarı yoluyla 11. ve 13. maddelere uygun olarak doğrulama kodu oluşturulması zorunludur.

Müşterinin yalnızca internet bankacılığı dağıtım kanalını kullanıyor olması ve mobil bankacılık dağıtım kanalını aktifleştirmemiş olması halinde ya da hem internet hem mobil bankacılık dağıtım kanalı aktif olmasına rağmen mobil bankacılık dağıtım kanalının mecburi bir sebepten ötürü müşteri tarafından kullanılamıyor olması halinde;

- **Login işlemlerinin gerçekleştirilmesinde**, müşterinin bildiği unsuru girmesini müteakip bilinen unsurun hash'i ile banka veritabanında şifreli olarak saklanan salted-hash değerleri karşılaştırılır, birbiriyle uyumlu ise login işlemine yönelik bir tek kullanımlık doğrulama kodu üretilerek SMS ile müşteriye iletilir ve müşterinin kendisine iletilen tek kullanımlık doğrulama kodunu ekrana girmesi sonrasında login işleminin gerçekleştirilmesi sağlanır.
- **Finansal sonuç doğuran işlemlerin gerçekleştirilmesinde,** öncelikle başarılı bir login sonrasında geçerliliğini koruyan bir oturumun bulunması zorunludur. Böyle bir oturum esnasında finansal sonuç doğuran bir işlem gerçekleştirilmek istenmesi halinde, işlem talebini alan bankanın bu işleme özgü olarak (alıcı ve tutar bilgisine spesifik olacak şekilde) tek kullanımlık bir doğrulama kodu üreterek SMS ile müşteriye iletmesi gerekmektedir. Müşterinin başarılı bir login sonrasında geçerliliğini koruyan bir oturum ekranından SMS ile kendisine iletilen tek kullanımlık doğrulama kodunu girmesi sonrasında, ilgili işlemin gerçekleştirilmesi sağlanır. **Ancak müşterinin her finansal sonuç doğuran işlem gerçekleştirme isteğinde bu sürecin tekrarlanması ve her işleme özgü yeni bir doğrulama kodunun müşteriye SMS ile gönderilerek, ekrana girilmesi zorunludur.**
- **Mobil bankacılık dağıtım kanalı aktif olmayan ve dolayısıyla "müşteriye özgü şifreleme gizli anahtarına" sahip olmayan bir müşterinin, yazılı şekle tabi bir sözleşme ilişkisini internet bankacılığı dağıtım kanalı üzerinden elektronik ortamda kurması mümkün bulunmamaktadır.**

- **Müşterinin mesafeli olarak sözleşme kurma talebini ve sözleşme kuran irade beyanını internet bankacılığı dağıtım kanalı üzerinden iletmesi mümkündür.** Bunun için öncelikle başarılı bir login sonrasında geçerliliğini koruyan bir oturumun bulunması zorunludur. Böyle bir oturum esnasında, müşterinin internet bankacılığı dağıtım kanalı üzerinden ya da başka bir kanal üzerinden ilettiği sözleşme kurma talebine özgü olarak bankanın tek kullanımlık bir doğrulama kodu üretmesi ve bunu SMS ile müşteriye iletmesi gerekmektedir. Müşterinin başarılı bir login sonrasında geçerliliğini koruyan bir oturum ekranında SMS ile kendisine iletilen doğrulama kodunu girmesi ve bu suretle mesafeli sözleşme kurmaya ilişkin irade beyanını bankaya iletmesi sağlanmalıdır.

Müşterinin hem mobil bankacılık dağıtım kanalının hem de internet bankacılığı dağıtım kanalının aktif olduğu ancak işlemlerin internet bankacılığından başlatıldığı hallerde,

- **Login işlemlerinin gerçekleştirilmesinde,** müşterinin bildiği unsuru girmesini müteakip bilinen unsurun hash'i ile banka veritabanında şifreli olarak saklanan salted-hash değerleri karşılaştırılır, birbiriyle uyumlu ise login işlemine yönelik olarak yukarıdaki **11. maddede belirtilen akışın uygulanması ve müşteriye özgü şifreleme gizli anahtarı ile imzalanacak şekilde bir doğrulama kodu oluşturulması sağlanır.**
- **Finansal sonuç doğuran işlemlerin gerçekleştirilmesinde,** öncelikle başarılı bir login sonrasında geçerliliğini koruyan bir oturumun bulunması zorunludur. Bu oturum esnasında finansal sonuç doğuran bir işlem gerçekleştirilmek istenmesi halinde, müşterinin internet bankacılığı dağıtım kanalından başlattığı işlemlerin öncelikle back-end sunucusuna iletilmesi ve back-end sunucusunun bu müşteri talebini doğrulanmak üzere uçtan uca güvenli kanaldan SS'e iletmesi gerekmektedir. Back-end'den SS'e müşteri talebinin iletilmesi sonrasında işlem talebini alan bankanın yukarıdaki **11. ve 13. maddede belirtilen akışı işletmesi gerekmektedir.**
- **Müşterinin yazılı şekle tabi bir sözleşme ilişkisi kurma sürecini internet bankacılığı dağıtım kanalı üzerinden başlatması mümkündür.** Bunun için öncelikle başarılı bir login sonrasında geçerliliğini koruyan bir oturumun bulunması zorunludur. Böyle bir oturum esnasında müşteri tarafından yazılı şekle tabi bir sözleşme ilişkisi kurulmasının istenmesi halinde, müşterinin internet bankacılığı dağıtım kanalından başlattığı bu isteğin öncelikle back-end sunucusuna iletilmesi ve back-end sunucusunun bu müşteri talebini doğrulanmak üzere uçtan uca güvenli kanaldan SS'e iletmesi gerekmektedir. Back-end'den SS'e müşteri talebinin iletilmesi sonrasında işlem talebini alan bankanın yukarıdaki **11. ve 13. maddede belirtilen akışı işletmesi gerekmektedir.**
- **Müşterinin mesafeli olarak sözleşme kurma talebini ve sözleşme kuran irade beyanını internet bankacılığı dağıtım kanalı üzerinden iletmesi mümkündür.** Bunun için öncelikle başarılı bir login sonrasında geçerliliğini koruyan bir oturumun bulunması zorunludur. Böyle bir oturum esnasında, müşterinin internet

bankacılığı dağıtım kanalı üzerinden ya da başka bir kanal üzerinden mesafeli olarak sözleşme ilişkisi kurmaya ilişkin ilettiği sözleşme kurma talebine yönelik olarak back-end sunucusunun bu müşteri talebini doğrulanmak üzere uçtan uca güvenli kanaldan SS'e iletmesi gerekmektedir. Back-end'den SS'e müşteri talebinin iletilmesi sonrasında işlem talebini alan bankanın yukarıdaki **11. ve 13. maddede belirtilen akışı işletmesi gerekmekte ve yazılı şekle tabi olmayan mesafeli bir sözleşme ilişkisi kuruluyor olsa bile müşteriye özgü şifreleme gizli anahtarı ile bu sözleşmeyi kuran irade beyanının imzalanması ve buna özgü bir doğrulama kodu oluşturulması gerekmektedir.**

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. **Diğer taraftan arayüz sağlayıcıların, mobil uygulama hizmet kanalı bulunmaksızın internet temelli hizmet kanalları üzerinden**

müşterilerine servis bankasının bankacılık hizmetlerini sunmaları mümkün bulunmamaktadır.

Bu itibarla, DBY uyarınca arayüz sağlayıcılığı faaliyetinde bulunacakların mobil uygulama hizmet kanalarının bulunması ve bu mobil uygulama arayüzü içinde, servis bankasının SDK'sının gömülü olması ve işbu Genelge ekinin 2.bölümünde belirtilen açıklamalara uygun olacak şekilde; 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 işlem imzalama akışlarının yürütülmesi zorunludur.

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, banka içi geliştirilen ya da satın alınan ürün ve hizmetlerin işbu Genelge ekinde yer verilen açıklamalara uygunluğunun sağlanması zorunludur.

Banka içi geliştirilen ya da satın alınan ürün ve hizmetlerin 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, **söz konusu ürün ve hizmetlerinin işbu Genelge ekinde yer verilen açıklamalara uygun olduğunu gösterecek ve Bankacılık Düzenleme ve Denetleme Kurumu tarafından yayımlanan Bankalarda Bilgi Sistemleri Denetimi Yapmaya Yetkili Bağımsız Denetim Kuruluşları listesinde yer alan bir bağımsız denetim kuruluşu tarafından hazırlanacak bir rapor ile 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.