Treasury and Trade Solutions

Security Procedures
Güvenlik Prosedürleri

1. Introduction
Giriş

These "Security Procedures", as referenced in the Communications section of the Master Account and Service Terms ("MAST") (or other applicable account terms and conditions), are designed to authenticate the Customer's log-on to the Bank's connectivity channels and to verify the origination of Communications between Bank and Customer in connection with the following Services or connectivity channels (the availability of which may vary across local markets).
Ana Hesap ve Hizmet Şartları ("AHHŞ") İletişim bölümünde (veya ilgili başka hesap şart ve koşullarında) referans gösterilen bu "Güvenlik Prosedürleri", Müşterinin Bankanın bağlantı kanallarında oturum açmasını doğrulamak ve aşağıdaki Hizmetlerle veya bağlantı kanallarıyla (kullanılabilirliği yerel pazarlarda değişiklik gösterebilmektedir) bağlantılı olarak Banka ve Müşteri arasındaki İletişimin oluşumunu teyit etmek amacıyla hazırlanmıştır.

- CitiDirect® (including WorldLink®)
  CitiDirect® (WorldLink® dahil)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Dünya Bankalararası Mali Telekomünikasyon Derneği ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Manuel Başlatılan Fon Transferi ("MIFT")
- Interactive Voice Response ("IVR")
  İnteraktif Sesli Yanıt ("IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
  Banka ile E-posta / Faks / Posta / Messenger / Telefon İletişimi
- Other local electronic connectivity channels
  Diğer yerel elektronik bağlantı kanalları

These Security Procedures are to be read together with the MAST and may be updated and advised to the Customer from time-to-time by electronic or other means, including but not limited to posting updates to the Security Procedures on CitiDirect. Unless otherwise provided by law, Customer's continued use of any of the above noted Services or connectivity channels after being advised of updated Security Procedures shall constitute Customer's acceptance of such updated Security Procedures. These Security Procedures cover the following:

Bu Güvenlik Prosedürleri AHHŞ ile birlikte yorumlanmalıdır ve zaman zaman güncellenebilir ve Güvenlik Prosedürleri güncellemelerinin CitiDirect'de yayınlanması dahil olmak, ancak bunlarla sınırlı olmamak üzere, elektronik veya başka yollarla Müşteriye bildirilebilir. Aksi mevzuatta öngörülmedikçe, Müşterinin yukarıda belirtilen Hizmetlerden veya bağlantı kanallarından herhangi birini, güncellenmiş Güvenlik Prosedürlerinin kendisine bildirilmesinden sonra kullanmaya devam etmesi, Müşterinin bu güncellenmiş Güvenlik Prosedürlerini kabul ettiği anlamına gelecektir. Bu Güvenlik Prosedürleri aşağıdakileri kapsar:

A. Authentication Methods
Kimlik Doğrulama Yöntemleri

B. Customer Responsibilities
Müşteri Sorumlulukları

C. Data Integrity and Secured Communications
Veri Bütünlüğü ve Güvenli İletişimler

D. Security Manager and Related Functions
Güvenlik Yöneticisi ve İlgili İşlevler

2. Authentication Methods
Kimlik Doğrulama Yöntemleri

The Security Procedures include certain secure authentication methods ("Authentication Methods") which are used to uniquely identify and verify the authority of the Customer and/or any of its users authorized by the Customer typically through one or a combination of mechanisms such as user ID/password pairs, digital certificates, biometrics, security tokens (deployed via hardware or software), seal/signature verification, and/or devices associated with the Authentication Methods (collectively, the "Credentials"). Authentication Methods and associated Credentials allow the Bank to verify the origin of Communications received by the Bank.

Güvenlik Prosedürleri, Müşterinin ve/veya Müşteri tarafından yetkilendirilmiş herhangi bir kullanıcısının tipik olarak kullanıcı kimliği/parola çiftleri, dijital sertifikalar, biyometrikler, şifre üreticileri (donanım veya yazılım aracılığıyla dağıtılan), mühür / imza doğrulaması ve/veya Kimlik Doğrulama Yöntemleriyle ilişkili aygıtlar (topluca "Kimlik Bilgileri") gibi bir mekanizma kombinasyonu ile yetkisini benzersiz bir şekilde tanımlamak ve doğrulamak için kullanılan belirli güvenli kimlik doğrulama yöntemlerini ("Kimlik Doğrulama Yöntemleri") içerir. Kimlik Doğrulama Yöntemleri ve ilişkili Kimlik Bilgileri, Bankanın, Banka tarafından alınan İletişimin kökenini doğrulamasına olanak tanır.

More information regarding Authentication Methods for access to Services and/or connectivity channels may be accessed on the CitiDirect Login Help website. Customer may at any time select an available Authentication Method. During implementation of Services or connectivity channels, Bank may set-up a default Authentication Method, which Customer may change at any time to another available Authentication Method.

Hizmetlere ve/veya bağlantı kanallarına erişime yönelik Kimlik Doğrulama Yöntemleri hakkında daha fazla bilgiye CitiDirect Oturum Açma Yardımı internet sitesi üzerinden ulaşabilirsiniz. Müşteri istediği zaman kullanılabilir bir Kimlik Doğrulama Yöntemi seçebilir. Hizmetlerin veya bağlantı kanallarının uygulanması sırasında Banka, Müşterinin istediği zaman mevcut başka bir Kimlik Doğrulama Yöntemiyle değiştirebileceği varsayılan bir Kimlik Doğrulama Yöntemi belirleyebilir.

The following Authentication Methods are available to access the services and/or connectivity channels:

Hizmetlere ve / veya bağlantı kanallarına erişmede aşağıdaki Kimlik Doğrulama Yöntemleri kullanılabilir:

CitiDirect Authentication Methods *CitiDirect Doğrulama Yöntemleri*	
Biometrics *Biyometrikler*	A digital authentication method that utilizes a user's unique physical traits, (such as a fingerprint and facial recognition), built-in biometric technology on the user's mobile device, and cryptographic techniques to gain access to CitiDirect. Physical trait data is not transferred to the Bank when the user selects this authentication method. *CitiDirect'e erişmek için kullanıcının benzersiz fiziksel özelliklerini (parmak izi ve yüz tanıma gibi), kullanıcının mobil cihazında yerleşik biyometrik teknolojiyi ve şifreleme tekniklerini kullanan dijital doğrulama yöntemi. Kullanıcı bu doğrulama yöntemini seçtiğinde fiziksel özellik verileri Bankaya aktarılmaz.*
Mobile Token (non-application based) *Mobil Token* *(uygulama tabanlı olmayan)*	A digital non-application based mobile authentication method (e.g. Mobile Token (App-less)) that leverages cryptographic keys and biometric authentication (such as fingerprint and facial recognition) to link a user's mobile device to their CitiDirect account via the user's mobile browser. Physical trait data is not transferred to the Bank when the user selects this authentication method. This method facilitates multi-factor authentication by verifying the user's identity with their registered mobile device. *Bir kullanıcının mobil cihazını, mobil tarayıcısı aracılığıyla CitiDirect hesabına bağlamak için şifreleme anahtarlarını ve biyometrik kimlik doğrulamayı (parmak izi ve yüz tanıma gibi) kullanan, uygulama tabanlı olmayan dijital bir mobil kimlik doğrulama yöntemi [örn. Mobil Token (Uygulamasız)]. Kullanıcı bu kimlik doğrulama yöntemini seçtiğinde fiziksel özellik verileri Bankaya aktarılmaz. Bu yöntem, çok faktörlü kimlik doğrulamayı, kullanıcının kimliğini kayıtlı mobil cihazıyla doğrulayarak gerçekleştirir.*
Challenge Response Token *Soru-Yanıt Belirteci*	Either (i) a mobile application based soft token (e.g. MobilePASS) or (ii) a physical token (e.g. SafeWord Card, Vasco), which in each case is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). When accessing CitiDirect, the system generates a challenge and a response passcode is generated by the utilized token and entered into the system. This authentication method, when combined with a secure password results in multifactor authentication. *Her durumda bir PİN (örn., 4 haneli bir PİN) ile doğrulandıktan sonra dinamik bir parola oluşturmada kullanılan ya (i) mobil uygulama bazlı yazılımsal bir belirteç (MobilePASS gibi) ya da (ii) fiziksel bir belirteç (SafeWord Card, Vasco gibi). CitiDirect'e erişirken, sistem bir soru oluşturur ve kullanılan belirteç tarafından bir soru ve bir yanıt parolası oluşturulur ve sisteme girilir. Bu doğrulama yöntemi, güvenli bir parola ile birleştirildiğinde çok faktörlü bir doğrulama elde edilir.*
One-Time Password Token *Tek Kullanımlık Şifre Belirteci*	Either (i) a mobile application based soft token (e.g. MobilePASS); or (ii) a physical token (e.g. SafeWord Card, Vasco) that is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). This dynamic password is entered into the system to gain access. *Bir PİN (örn., 4 haneli bir PİN) ile doğrulandıktan sonra dinamik bir şifre oluşturmada kullanılan ya (i) mobil uygulama bazlı yazılımsal bir belirteç (MobilePASS gibi) ya da (ii) fiziksel bir belirteç (SafeWord Card, Vasco gibi). Bu dinamik şifre, erişim sağlamak için sisteme girilir.*

CitiDirect Authentication Methods ***CitiDirect Doğrulama Yöntemleri***	
Secure Password *Güvenli Parola*	A user enters his or her secure password to access the system. A secure password typically limits a user's capabilities on the system, for example, by only permitting that certain information be viewed by the user. This authentication method, when combined with a challenge response token results in multifactor authentication. *Kullanıcı, sisteme erişmek için güvenli parolasını girer. Güvenli parola, kullanıcının sistem üzerindeki yetkilerini sınırlandırarak, örneğin yalnızca belirli bilgilerin görüntülenmesine izin verilmesini sağlar. Bu doğrulama yöntemi, güvenli bir soru-yanıt belirteci ile birleştirildiğinde çok faktörlü bir kimlik doğrulaması elde edilir.*
SMS One-Time Code *SMS Tek Kullanımlık Şifre*	A dynamic password delivered to users via SMS, after which the user enters the dynamic password and a secure password to gain access to the system. *Dinamik şifre, SMS ile kullanıcıya gönderilir ve ardından kullanıcı, sisteme erişim sağlamak için dinamik şifreyi ve güvenli parolayı sisteme girer.*
Voice One-Time Code *Sesli Tek Kullanımlık Şifre*	A dynamic password delivered to users via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system. *Tek kullanımlık dinamik şifre, kullanıcıya otomatik bir sesli arama yoluyla iletilir. Kullanıcı, bu şifreyi güvenli parolasıyla birlikte sisteme girerek erişim sağlar.*
Digital Certificates *Dijital Sertifikalar*	A digital certificate is an electronic identification issued by an approved certificate authority for authentication and authorization. Digital certificates may be attributed to corporate legal entities ("Corporate Seals") or individuals ("Personal Certificates"). The Customer is responsible for properly verifying the identity of all users of Personal Certificates acting on behalf of the Customer in accordance with local law. The Bank and the Customer are required to use digital certificates provided by authorized persons, to ensure all Communications exchanged via a public Internet connection or an otherwise unsecure Internet connection are fully encrypted and protected. *Dijital sertifika, doğrulama ve yetkilendirme için onaylı bir sertifikalandırma makamı tarafından verilen elektronik kimliktir. Dijital sertifikalar kurumsal tüzel kişilere ("Şirket Kaşeleri") veya gerçek kişilere ("Kişisel Sertifikalar") verilebilir. Müşteri, yerel yasalara uygun olarak Müşteri adına hareket eden tüm Kişisel Sertifika kullanıcılarının kimliklerinin doğru bir şekilde doğrulanmasından sorumludur.* *Banka ve Müşteri, halka açık bir İnternet bağlantısı veya güvenli olmayan bir İnternet bağlantısı üzerinden yapılan tüm İletişimlerin tamamen şifrelenmesini ve korunmasını sağlamak için yetkili kişiler tarafından sağlanan dijital sertifikaları kullanmakla yükümlüdür.*

CitiConnect for Files Authentication Methods *Methods CitiConnect for Files Doğrulama*	
Digital Certificates *Dijital Sertifikalar*	See description above. *Yukarıdaki açıklamaya bakın.*

CitiConnect for Files Authentication Methods *Methods CitiConnect for Files Doğrulama*	
IP Address Whitelist When Using CitiConnect *CitiConnect Kullanırken Güvenli IP Adresi Listesi*	Certain Internet communications received by the Bank, for example, via a Virtual Private Network (VPN), may also rely on the parties exchanging information using pre-agreed Internet Protocol (IP) addresses. The Bank will only accept communications originating from the Customer's designated IP address, and vice versa; and the Bank will only transmit Communications to the Customer's designated IP address, and vice versa. Used in conjunction with Digital Certificate method above. *Banka tarafından, örneğin bir Sanal Özel Ağ (VPN) aracılığıyla, alınan belirli İnternet iletişimlerinde, önceden kararlaştırılmış İnternet Protokolü (IP) adreslerini kullanarak bilgi alışverişinde bulunan taraflara da dayanılabilir. Banka ve Müşteri, sadece belirledikleri IP adresinden gelen iletişimleri kabul edecek ve iletişimleri sadece belirledikleri IP adresine gönderecektir. Yukarıdaki Dijital Sertifika yöntemi ile birlikte kullanılır.*

CitiConnect API Authentication Methods ***CitiConnect API Doğrulama Yöntemleri***	
Digital Certificates *Dijital Sertifikalar*	See description above. *Yukarıdaki açıklamaya bakın.*
IP Address Whitelist When Using CitiConnect *CitiConnect Kullanırken Güvenli IP Adresi Listesi*	See description above. *Yukarıdaki açıklamaya bakın.*

CitiConnect for SWIFT Authentication Methods ***CitiConnect for SWIFT Doğrulama Yöntemleri***	
Digital Certificates *Dijital Sertifikalar*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Yukarıdaki açıklamaya bakın. Aşağıdaki SWIFT doğrulama yöntemi ile birlikte kullanılabilir.*

CitiConnect for SWIFT Authentication Methods *CitiConnect for SWIFT Doğrulama Yöntemleri*	
SWIFT Authentication *SWIFT Kimlik Doğrulaması*	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWIFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications. The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT. Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards. *Banka ve Müşteri arasında SWIFT ağı aracılığıyla gönderilen, hesap bilgileri, ödeme emirleri ve bu tür emirleri değiştirme veya iptal etme talimatlarını içeren, ancak bunlarla da sınırlı olmayan iletişimler,Genel Şart ve Koşulları ve FIN Hizmet Tanımını içeren, ancak bunlarla da sınırlı olmayan SWIFT'in Sözleşme Belgelerinde (zaman tadil edildiği veya takviye edildiği şekliyle) tanımlanan veya SWIFT tarafından oluşturulabilecek diğer şartlarda ve koşullarda düzenlenen prosedürler kullanılarak doğrulanacaktır. Banka, bu İletişimlerin göndericisini ve doğruluğunu belirlemek için SWIFT prosedürlerinde yer alanlardan başka bir şey yapmak zorunda değildir.* *Banka, SWIFT sistemindeki hata veya gecikmelerden sorumlu değildir. Müşteri, iletişimleri Bankaya SWIFT tarafından istenen ve belirtilen format ve tipte göndermekle sorumludur.* *SWIFT olanakları aracılığıyla gönderilen veya alınan iletimler ve iletişimleri, üyelik kuralları da dâhil olmak üzere yürürlükteki SWIFT kurallarına ve düzenlemelerine tabidir. Müşteri, SWIFT mesajlaşma standartlarını bilmek ve bunlara uymakla sorumludur.*

SWIFT Authentication Method ***SWIFT Doğrulama Yöntemi***	
SWIFT Authentication (Direct Connection for Financial Institutions) *SWIFT Doğrulama (Finansal Kurumlar için Doğrudan Bağlantı)*	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWIFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications. The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT. Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards. *Banka ve Müşteri arasında SWIFT ağı aracılığıyla gönderilen, hesap bilgileri, ödeme emirleri ve bu tür emirleri değiştirme veya iptal etme talimatlarını içeren, ancak bunlarla da sınırlı olmayan iletişimler, Genel Şart ve Koşulları ve FIN Hizmet Tanımını içeren, ancak bunlarla da sınırlı olmayan SWIFT'in Sözleşme Belgelerinde (zaman tadil edildiği veya takviye edildiği şekliyle) tanımlanan veya SWIFT tarafından oluşturulabilecek diğer şartlarda ve koşullarda düzenlenen prosedürler kullanılarak doğrulanacaktır. Banka, bu İletişimlerin göndericisini ve doğruluğunu belirlemek için SWIFT prosedürlerinde yer alanlardan başka bir şey yapmak zorunda değildir.* *Banka, SWIFT sistemindeki hata veya gecikmelerden sorumlu değildir. Müşteri, iletişimleri Bankaya SWIFT tarafından istenen ve belirtilen format ve tipte göndermekle sorumludur.* *SWIFT olanakları aracılığıyla gönderilen veya alınan iletimler ve iletişimleri, üyelik kuralları da dahil olmak üzere yürürlükteki SWIFT kurallarına ve düzenlemelerine tabidir. Müşteri, SWIFT mesajlaşma standartlarını bilmek ve bunlara uymakla sorumludur.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Dijital/ Elektronik İmza Elektronik Belge Gönderimi İçin Doğrulama Yöntemleri***	
Digital Signature *Dijital İmza*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *İmza, mesaj, yazılım veya dijital belgenin doğruluğunu ve bütünlüğünü doğrulamak için dijital sertifikalardan yararlanan bir elektronik imza türü.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Dijital/ Elektronik İmza Elektronik Belge Gönderimi İçin Doğrulama Yöntemleri***	
Electronic Signature *Elektronik İmza*	An electronic symbol attached to a contract or other record, unique to and used by a person with an intent to sign. Electronic signatures can be established in the form of words, letters, numerals, symbols, click of a button on a website, upload of facsimile or scan of a physical signature, signing on a touchscreen, or agreeing to any terms and conditions by electronic means. Created under the sole control of the person using it, it is logically attached to or associated with a data message, capable of identifying the person who consents to the data message and certifying the person's consent. Such Electronic Signature would be submitted to the Bank through the Bank's electronic channels and in compliance with the associated Authentication Methods described above. *İmzalama niyetiyle hareket eden kişiye özgü olarak kullanılan ve bir sözleşmeye veya başka bir kayda eklenen elektronik bir semboldür. Elektronik imzalar; sözcükler, harfler, rakamlar veya semboller kullanılarak, bir web sitesindeki butona tıklayarak, faks veya taranmış ıslak imza yükleyerek, dokunmatik ekrana imza atarak ya da herhangi bir şart ve koşulu elektronik ortamda onaylayarak oluşturulabilir. Kullanan kişinin kontrolü altında oluşturulan elektronik imza, veri mesajına izin veren kişinin kimliğini tespit edebilen ve kişinin iznini tasdik edebilen bir veri mesajına mantıksal olarak eklenir veya bu veri mesajı ile ilişkilendirilir. Bu Elektronik İmza, Bankanın elektronik kanalları aracılığıyla ve yukarıda açıklanan ilgili Doğrulama Yöntemlerine uygun olarak Bankaya sunulacaktır.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Method Manuel Başlatılan Fon Transferi ("MBFT") Doğrulama Yöntemi***	
MIFT Authentication *MBFT Doğrulaması*	Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancelations of previous manual instructions, may be made by fax or letter or upload to CitiDirect. Not all forms are supported in all countries. Initiators are persons designated by the Customer who are authorized to initiate transactions in accordance with restrictions, if any, are identified by the Customer. Confirmers are person designated by the Customer that Bank may call back, at its discretion, for confirmation of manually initiated instructions for funds transfers. In certain countries, mobile telephone numbers are not accepted as call back numbers. Further details are provided in the applicable Country Cash Management User Guide, Global Manual Transaction Authorization or Universal Nomination Form. MIFT is to be used by the Customer as a contingency method to communicating instructions to the Bank. *Önceki manuel talimatlarda yapılan değişiklikler, geri arama veya talimat iptalleri dâhil olmak üzere Manuel Başlatılan Fon Transferi ("MBFT"), faks veya mektup veya CitiDirect'e yükleme yoluyla yapılabilir. Tüm formlar tüm ülkelerde desteklenmemektedir. Başlatıcılar, Müşteri tarafından belirlenen ve varsa Müşteri tarafından tanımlanan kısıtlamalara uygun olarak işlem başlatmayı yetkili olan kişilerdir. Onaylayanlar, Müşteri tarafından belirlenen ve Bankanın kendi takdirine bağlı olarak, para transferlerine ilişkin manuel başlatılan talimatların onaylanması için geri arayabileceği kişilerdir.* *Bazı ülkelerde cep telefonu numaraları geri arama numarası olarak kabul edilmemektedir. Diğer ayrıntılar, ilgili Ülke Nakit Yönetimi Kullanıcı Kılavuzu, Küresel Manuel İşlem Yetkisi veya Evrensel Aday Gösterme Formunda verilmiştir. MBFT, Müşteri tarafından Bankaya talimatların iletilmesinde bir acil durum yöntemi olarak kullanılacaktır.*

Mail, Fax, Email and Messenger Authentication Methods ***Posta, Faks, E-posta ve Messenger Doğrulama Yöntemleri***	
Seal Image Verification *Mühür Görüntü Doğrulaması*	Correspondence received by the Bank via fax, mail, email or messenger, excluding MIFT requests, are verified and collated with due care based on the seal image contained in the Customer's authority document or similar document provided to the Bank. *MBFT talepleri hariç olmak üzere, Banka tarafından faks, posta, e-posta veya haberci yoluyla alınan yazışmalar, Müşterinin yetki belgesinde yer alan mühür görüntüsü veya Bankaya sağlanan benzer bir belge esas alınarak gerekli özen gösterilerek doğrulanır ve karşılaştırılır.*
Signature Verification *İmza Doğrulama*	Correspondence received by the Bank via fax, mail email or messenger, excluding MIFT requests, are signature verified based on the information contained in the Customer's authority document or similar document provided to the Bank. *MBFT talepleri hariç olmak üzere, Banka tarafından faks, posta e-postası veya mesajlaşma yoluyla alınan yazışmalar, Müşterinin yetki belgesinde yer alan imza veya Bankaya sağlanan benzer bir belge esas alınarak doğrulanır.*
Secure PDF *Güvenli PDF*	Encrypted emails are delivered to a regular mailbox as PDF documents that are opened by entering a private password. Both the message body and any attached files are encrypted. A private password can be set up upon receipt of the first secure email received. *Şifrelenmiş e-postalar, özel bir parola girilerek açılan PDF belgeleri olarak normal bir posta kutusuna teslim edilir. Hem ileti gövdesi hem de ekli dosyalar şifrelenir. İlk güvenli e-postanın alınması üzerine özel bir şifre ayarlanabilir.*
MTLS *Zorunlu Taşıma Katmanı Güvenliği*	Mandatory Transport Layer Security (MTLS) creates what would be a secure, private email connection between the Bank and the Customer. Emails transmitted using this channel are sent over the Internet through an encrypted TLS tunnel created by the connection. *Zorunlu Taşıma Katmanı Güvenliği (MTLS), Banka ile Müşteri arasında güvenli, özel bir e-posta bağlantısı oluşturur. Bu kanal kullanılarak iletilen/gönderilen e-postalar, İnternet üzerinden, bu bağlantı tarafından oluşturulan şifreli bir TLS tüneli aracılığıyla gönderilir.*

Phone Authentication Methods ***Telefon Doğrulama Yöntemleri***	
PIN *PIN Kodu*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Banka ile telefonla iletişim kuran müşterilerden, yetkilendirilmiş erişimlerini doğrulamaları için bir PİN girmeleri istenir.*
Verification Questions *Doğrulama Soruları*	Customers contacting the Bank via phone are prompted by the Bank's service representatives to provide correct verbal responses to verification questions in order to validate authorized access. *Banka ile telefonla iletişim kuran müşterilerden, Banka hizmet temsilcileri tarafından yetkilendirilmiş erişimlerini doğrulamaları için doğrulama sorularına doğru sözlü yanıtlar vermeleri istenir.*

The availability of Authentication Methods described above varies based on local markets.
Yukarıda açıklanan Kimlik Doğrulama Yöntemlerinin kullanılabilirliği yerel pazarlara göre değişiklik göstermektedir.

3. Customer Responsibilities
Müşteri Sorumlulukları

3.1 Identifying Authorized Users: Customer is responsible for identifying: (i) all individuals acting on the Account(s) on behalf of the Customer at an entity level for all Services and connectivity channels, and (ii) each person acting on behalf of the Customer being duly authorized by the Customer to act on the Customer's Account.

Yetkili Kullanıcıları Tanımlama: Müşteri, (i) Hesap/Hesaplar ile ilgili olarak tüm Hizmetler ve bağlantı kanallarında tüzel bir kişi düzeyinde Müşteri adına hareket eden tüm kişileri ve (ii) Müşteri Hesabı ile ilgili hareket etmeye Müşteri tarafından tam yetkilendirilmiş olarak Müşteri adına hareket eden her bir kişiyi belirlemekle sorumludur.

3.2 Customer is responsible for assigning and monitoring any transaction limits assigned to the Customer and/ or its users and ensuring that these limits (a) do not exceed the limits as required by the Customer's internal policies and other authority and constitutive documents such as Customer's Board of Director resolutions, Bank Mandates, Power Of Attorney, or equivalent document, and (b) are properly reflected on all connectivity channels and user entitlements.

Müşteri, Müşteriye ve/veya kullanıcılarına tahsis edilen işlem limitlerini tayin etmek ve izlemek ve bu limitlerin (a) Müşterinin iç politikaları ile Müşterinin Yönetim Kurulu kararları, Banka Direktifleri, Vekaletname veya eşdeğeri bir belge gibi diğer yetki ve kurucu belgelerinin gerektirdiği sınırları aşmamasını ve (b) tüm bağlantı kanallarına ve kullanıcı haklarına gerektiği şekilde yansıtılmasını sağlamakla sorumludur.

3.3 Certain jurisdictions may require individuals (and their corresponding Credentials) to be identified by the Bank in accordance with applicable AML legislation requirements before granting access to perform certain functions. Please contact your Customer Service Representative or visit the CitiDirect website for further information.

Bazı ülkeler, kişilerin (ve karşılık gelen kimlik bilgilerinin) belirli işlevleri yerine getirmeleri için kendilerine erişim izni verilmeden önce yürürlükteki Kara Para Aklamanın Önlenmesi mevzuatı şartlarına uygun olarak Banka tarafından tespit edilmesini öngörmektedir. Lütfen daha fazla bilgi için Müşteri Hizmetleri Temsilcinize başvurun veya CitiDirect'in internet sitesini ziyaret edin.

3.4 Safeguarding of Authentication Methods
Kimlik Doğrulama Yöntemlerinin Korunması

The Customer is responsible for safeguarding the Authentication Methods and Credentials with the highest standard of care and diligence, and ensuring that access to and distribution of the Credentials are limited only to persons that have been authorized by the Customer.

Communications sent by a third party: Where the Customer is using a Credential to identify and authenticate their Communications as originating from them as a legal entity, the Customer is responsible for exercising full control over the use of such Credentials when sending Communications to the Bank, including where such Communications are sent by applications and/or systems that are managed by a third party on behalf of the Customer. In all circumstances the Bank will (a) deem any Communication it receives through an electronic connectivity channel, that has been received by the Bank in compliance with these Security Procedures duly authenticated as originating from the Customer, as a Communication instructed by the Customer and (b) may act upon any Communication that it receives on behalf of the Customer in compliance with these Security Procedures.

Müşteri, Kimlik Doğrulama Yöntemlerini ve Kimlik Bilgilerini en yüksek standartta özen ve titizlikle korumak ve Kimlik Bilgilerine erişimin ve bunların dağıtımının yalnızca Müşteri tarafından yetkilendirilmiş kişilerle sınırlı olmasını sağlamakla sorumludur.

Üçüncü taraflarca gönderilen iletişimler: Müşterinin, tüzel bir kişi olarak kendisi tarafından gönderilen İletişimlerini tanımlamak ve doğrulamak için bir Kimlik Bilgisini kullandığı durumlarda, bu İletişimlerin Müşteri adına üçüncü bir tarafça yönetilen uygulamalar ve / veya sistemler aracılığıyla nerelere gönderildiği de dahil olmak üzere, İletişimleri Bankaya gönderilen bu Kimlik Bilgilerinin kullanımı üzerinde tam kontrol sağlamakla sorumludur. Her koşulda, Banka, Müşteri tarafından gönderildiği gerektiği şekilde doğrulanarak Banka tarafından bu Güvenlik Prosedürlerine

uygun olarak alınmış olan, elektronik bir bağlantı kanalı aracılığıyla aldığı her tür İletişimi Müşteri tarafından talimat verilen bir İletişim olarak kabul edecek ve (b) Müşteri adına aldığı her tür İletişim konusunda bu Güvenlik Prosedürlerine uygun olarak hareket edebilir.

4. Data Integrity and Secured Communications *Veri Bütünlüğü ve Güvenli İletişimler*

4.1 The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the internet, mail, email and/or fax which the Customer understands are not (i) necessarily secure communications and delivery systems, and (ii) under the Bank's control. The Customer further understands that if Customer's users are entitled to access Open Banking and/or similar third-party platforms outside of the Citi systems, Customer data could be transmitted over such third-party platforms which are not under the Bank's control.

Müşteri, Bankaya veri aktarırken ve Bankayla iletişim kurarken internet, posta, e-posta ve/veya faks kullanacak olup bunların (i) mutlaka güvenli iletişim ve dağıtım sistemleri olmadığını ve (ii) Bankanın kontrolü altında olduğunu kabul eder. Müşteri ayrıca, Müşterinin kullanıcılarının Açık Bankacılık ve/veya Citi sistemleri dışındaki benzeri üçüncü taraf platformlara erişim hakkına sahip olması durumunda, Müşteri verilerinin Bankanın kontrolü altında olmayan söz konusu üçüncü taraf platformlar üzerinden aktarılabileceğini kabul eder.

4.2 The Bank, utilizes industry leading encryption methods (as determined by the Bank), which help to ensure that information is kept confidential and that it is not changed during electronic transit.

Banka, bilgilerin gizli tutulmasını ve elektronik iletim sırasında değiştirilmemesini sağlamaya yardımcı sektörün önde gelen şifreleme yöntemlerini (Banka tarafından belirlenen) kullanmaktadır.

4.3 If the Customer suspects or becomes aware of a technical failure or any improper or potentially fraudulent access to or use of the Bank's Services or connectivity channels or Authentication Methods by any person (whether an authorized person or not), the Customer shall promptly notify the Bank of such occurrence. In the event of improper or potentially fraudulent access or use by an authorized person, the Customer should take immediate actions to terminate such authorized person's access to and use of the Bank's Services or connectivity channels.

Müşteri, Banka Hizmetlerinden veya bağlantı kanallarından veya Kimlik Doğrulama Yöntemlerinden herhangi birinde teknik bir arıza olduğundan ya da (yetkili olsun ya da olmasın) herhangi bir kişi tarafından uygunsuz şekilde kullanıldığından veya bunlara potansiyel olarak hileli erişildiğinden şüphelenmesi veya haberdar olması halinde, durumu derhal Bankaya bildirecektir. Yetkili bir kişinin bunlara yetkisiz veya hileli erişim sağlaması veya bunları uygunsuz kullanması durumunda, Müşteri, bu yetkili kişinin Banka Hizmetlerine veya bağlantı kanallarına erişimini ve kullanımını iptal etmek için gerekli adımları derhal alacaktır.

4.4 If the Customer utilizes file formatting or encryption software (whether provided by the Bank or a third party) to support the formatting and recognition of the Customer's data and instructions and acts upon Communications with the Bank, the Customer will use such software solely for the purpose for which it has been installed.

Müşterinin, Müşteri verilerinin ve talimatlarının biçimlendirilmesini ve tanınmasını desteklemek için (Banka ya da üçüncü bir tarafça sağlanan) dosya biçimlendirme, şifreleme yazılımları kullanıyor ve Banka ile arasındaki iletişimlere göre hareket ediyor olması durumunda, Müşteri bu yazılımları sadece kuruldukları amaç doğrultusunda kullanacaktır.

4.5 The Customer accepts that the Bank may suspend or deny users' access to Services requiring the use of Credentials (i) in case of suspicion of unauthorized or fraudulent use of the Credentials and/or (ii) to safeguard the Services or Credentials.

Müşteri, (i) Kimlik Bilgilerinin yetkisiz veya hileli bir şekilde kullanıldığından şüphelenilmesi durumunda ve/veya (ii) Hizmetlerin ve/veya Kimlik Bilgilerinin korunması amacıyla Bankanın kullanıcıların, Kimlik Bilgilerinin kullanımını gerektiren Hizmetlere erişimini askıya alabileceğini veya reddedebileceğini kabul eder.

5. Security Manager and Related Functions
Güvenlik Yöneticisi ve İlgili İşlevler

For applications accessible in CitiDirect and CitiConnect (with the exception of Personal Certificates discussed below), the Bank requires the Customer to establish a "Security Manager" function. Security Managers are responsible for:

CitiDirect ve CitiConnect'de erişilebilen uygulamalar için (aşağıda ele alınan Kişisel Sertifikalar hariç) Banka, Müşteriden bir "Güvenlik Yöneticisi" işlevi tesis etmesini talep eder. Güvenlik Yöneticileri aşağıda sıralananlardan sorumludur:

5.1 Establishing and maintaining the access and entitlements of users (including Security Managers themselves) including activities such as: (a) creating, deleting or modifying user Profiles (including Security Manager Profiles) and entitlement rights (Note that user name must align with supporting identification documents); (b) building access profiles that define the functions and data available to individual users; (c) enabling and disabling user log-on credentials; and (d) assigning transaction limits (Note these limits are not monitored or validated by the Bank and Customer should monitor these limits to ensure they are in compliance with the Customer's internal policies and requirements, including but not limited to, those established by the Customer's Board of Directors or equivalent);

(a) kullanıcı Profilleri (Güvenlik Yöneticisi Profilleri dâhil) ve yetkilendirme hakları oluşturma, silme veya değiştirme (Kullanıcı adının destekleyici kimlik belgelerine uygun olması gerektiğini unutmayın), (b) bireysel kullanıcılar için mevcut olan fonksiyonları ve verileri tanımlayan erişim profilleri oluşturma, (c) kullanıcı oturum açma kimlik bilgilerini etkinleştirme ve devre dışı bırakma ve (d) işlem limitleri tayin etmek (Bu limitlerin Banka tarafından izlenmediğini veya doğrulanmadığını ve Müşterinin, Müşteri Yönetim Kurulu veya eşdeğer, tarafından belirlenenler de dâhil olmak, ancak bunlarla sınırlı olmamak üzere, Müşterinin dâhili politikalarına ve gereksinimlerine uygun olmalarını sağlamak için bu limitleri izlemesi gerektiğini unutmayın) gibi faaliyetler de dâhil olmak üzere kullanıcıların (Güvenlik Yöneticileri dâhil) erişim ve yetkilerini oluşturmak ve devam ettirmek,

5.2 Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same;

Müşteri nezaretindeki kütüphanelerde (önceden biçimlendirilmiş ödemeler ve lehtar kütüphaneleri gibi) girdiler oluşturma ve değiştirme ve diğer kullanıcıların bunları yapmalarına izin verme,

5.3 Modifying payment authorization flows;

Ödeme yetkilendirme akışlarını değiştirme,

5.4 Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users;

Dinamik parola bilgileri veya diğer sistem erişim bilgileri veya parolalarını Müşteri kullanıcılarına tahsis etme ve

5.5 Notifying the Bank, if there is any reason to suspect that security has been compromised; and

Güvenliğin tehlikeye girdiğinden şüphelenmek için herhangi bir neden olduğunda Bankaya bildirimde bulunma.

5.6 Managing and procuring digital certificates and authorizing other users to do the same.

Dijital sertifikaların temini ve yönetimi ile diğer kullanıcıları bu işlemleri yapabilmeleri için yetkilendirme.

Please note: Security Manager roles and responsibilities may vary or not be applicable in certain markets due to regulatory requirements and/or operational capabilities. In such markets, the Bank may require additional documentation and other information from the Customer to perform Security Manager functions on behalf of the Customer.

Önemli not: Güvenlik Yöneticisi görevleri ve sorumlulukları, düzenleyici şartlar ve / veya operasyonel yetenekler nedeniyle bazı pazarlarda değişiklik gösterebilir veya uygulanmayabilir. Bu tür pazarlarda Banka, Güvenlik Yöneticisi işlevlerini Müşteri adına yerine getirmek için Müşteriden ek belgeler ve başka bilgiler isteyebilir.

6. Use of CitiDirect and CitiConnect by Security Managers *CitiDirect ve CitiConnect'in Güvenlik Yöneticileri Tarafından Kullanımı*

The Bank requires two (2) separate individuals to input and authorize instructions; therefore, a minimum of two Security Managers are required. Any two Security Managers, acting in concert, are able to give instructions and/or confirmations through the connectivity channels in relation to any Security Manager function or in connection with facilitating communications. Any such communications, when authorized by two Security Managers, will be accepted and acted on by the Bank and deemed to be given by the Customer. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate Customer's Security Managers on the TTS Channels Onboarding Form. A Security Manager of the Customer may also act as the Security Manager for a third party entity (for instance, an affiliate of the Customer) and exercise all rights relating thereto (including the appointment of users for that third party entity's Account(s)), without any further designation, if that third party entity executes a Universal Access Authority form (or such other form of authorization acceptable to the Bank) granting the Customer access to its account(s). This only applies in relation to Account(s) covered under the relevant authorization.

Banka, talimatların girilmesi ve bu talimatlara onay verilmesi için iki ayrı kişi öngörmektedir ve bu nedenle en az iki Güvenlik Yöneticisi gereklidir. Birlikte hareket eden iki Güvenlik Yöneticisi, herhangi bir Güvenlik Yöneticisi işleviyle ilgili veya iletişimlerin kolaylaştırılmasıyla bağlantılı olarak bağlantı kanalları üzerinden talimatlar ve/veya onaylar verebilir. Bu iletişimler, iki Güvenlik Yöneticisi tarafından onaylandığında Banka tarafından kabul edilir ve Banka bunların gereğini yerine getirir ve Müşteri tarafından verilmiş kabul edilir. Banka, yeterli desteğin sağlanması için en az üç Güvenlik Yöneticisinin görevlendirilmesini tavsiye eder. Müşteri, kendi Güvenlik Yöneticilerini TTS Kanalları İşe Alım ve İşe Alıştırma Formu üzerinde tayin edecektir. Müşterinin Güvenlik Yöneticisi başkaca bir görevlendirme olmaksızın aynı zamanda üçüncü taraf bir işletmenin (örneğin, Müşterinin bağlı bir şirketi) Güvenlik Yöneticisi olarak hareket edebilir ve bunlarla ilgili tüm hakları (bu üçüncü taraf işletmesinin Hesabı/Hesapları için kullanıcıların atanması dâhil) kullanabilir ancak bunun için bu üçüncü taraf işletmesinin Müşteriye Hesabına/Hesaplarına erişim izni veren Evrensel Erişim Yetkisi Formu (veya Banka tarafından kabul edilebilir başka bir yetkilendirme formu) düzenlemesi gerekir. Bu sadece ilgili yetkilendirmenin kapsadığı Hesap/Hesaplar ile ilgili olarak geçerlidir.

7. Use of CitiDirect by Security Officers (For Personal Certificates only) *CitiDirect'in Güvenlik Görevlileri Tarafından Kullanımı (Sadece Kişisel Sertifikalar İçin)*

The Bank requires two (2) separate individuals to manage digital certificates attributed to individuals ("Personal Certificates"). Therefore, two Security Officers are required to assign and removal Personal Certificates to users, for the purpose of authenticating and authorizing Communications on the connectivity channels. The Bank recommends the designation of at least three Security Officers to ensure adequate backup. Any Communications authorized by Personal Certificates will be accepted and acted on by the Bank and deemed to be given by the Customer.

Banka, bireylere atfedilen dijital sertifikaların ("Kişisel Sertifikalar") yönetilmesi için iki (2) ayrı kişinin bulunmasını zorunlu kılar. Bu nedenle, bağlantı kanalları üzerindeki İletişimlerin kimliğini doğrulamak ve yetkilendirmek amacıyla, kullanıcılara Kişisel Sertifikaları atamak ve kaldırmak için iki Güvenlik Görevlisi gereklidir. Banka, yeterli yedeklemeyi sağlamak adına en az üç Güvenlik Görevlisinin görevlendirilmesini tavsiye eder. Kişisel Sertifikalar ile yetkilendirilen her türlü İletişim, Banka tarafından kabul edilecek, işleme konulacak ve Müşteri tarafından verilmiş addedilecektir.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions

© 2025 Citibank, N.A. Citi, Citi and Arc Design and other marks used herein are service marks of Citigroup Inc. or its affiliates, used and registered throughout the world.
1982580 10/25