Treasury and Trade Solutions

Security Procedures
Biztonsági eljárások

1. Introduction
Bevezetés

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).

Jelen „Biztonsági eljárások" célja, amint az a Globális Pénzforgalmi és Szolgáltatási Feltételek („MAST") (vagy a számlára vonatkozó egyéb érvényes feltételek) Üzenetváltásról szóló részében is szerepel, hogy meghatározza az Ügyfél hozzáférési feltételeit a Bank elektronikus csatornáihoz, továbbá, hogy meghatározza, ki és milyen feltételekkel jogosult az alábbi szolgáltatásokkal és kapcsolatot biztosító csatornákkal (amelyek elérhetősége országonként változhat) összefüggésben megbízást kezdeményezni a Bank és az Ügyfél között.

- CitiDirect® (including WorldLink®)
  CitiDirect® (beleértve a WorldLink®-et)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság – Society for Worldwide Interbank Financial Telecommunication („SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Manuális úton kezdeményezett átutalási megbízások – Manually Initiated Funds Transfer („MIFT")
- Interactive Voice Response ("IVR")
  Hangalapú szolgáltatás – Interactive Voice Response („IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
  E-mail/telefax/postai levélváltás/Messenger/telefonhívás a Bankkal
- Other local electronic connectivity channels
  Egyéb helyi elektronikus kapcsolódási csatornák

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:

A Biztonsági eljárásokat a MAST feltételeivel együtt kell értelmezni, és az esetleges módosításokról az Ügyfelet elektronikus vagy egyéb úton értesíteni kell, ideértve többek között a Biztonsági eljárások változásainak közzétételét a CitiDirect-en. A hatályos jogszabályok ettől eltérő rendelkezése hiányában, ha az Ügyfél a Biztonsági eljárások módosulásáról szóló értesítést követően továbbra is igénybe veszi a fenti szolgáltatásokat vagy kapcsolatot biztosító csatornákat, azt úgy kell tekinteni, hogy elfogadta a módosított Biztonsági eljárásokat. Jelen Biztonsági eljárások az alábbiakat szabályozzák:

A. Authentication Methods
Hitelesítési módszerek

B. Customer Responsibilities
Az Ügyfél kötelezettségei

C. Data Integrity and Secured Communications
Adatintegritás és biztonságos üzenetváltás

D. Security Manager and Related Functions
Rendszeradminisztrátor feladata és felelősségi körei

2. Authentication Methods *Hitelesítési módszerek*

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.

A Biztonsági eljárások olyan biztonságos hitelesítési módszereket (Hitelesítési módszerek") tartalmaznak, amelyek segítségével egyedileg azonosítható az Ügyfél és/vagy bármely felhasználója, jellemzően olyan mechanizmus vagy olyan mechanizmusok kombinációja által, mint a felhasználó azonosító/jelszó párosítás, digitális tanúsítványok, biometrikus jellemzők, (fizikai vagy szoftver-alapú) biztonsági eszközök, bélyegző/aláírás ellenőrzése és/vagy a Hitelesítési módszerekhez kapcsolódó eszközök (együttesen: „Hitelesítési adatok"). A Hitelesítési módszerek és a hozzájuk kapcsolódó Hitelesítési adatok segítségével a Bank ellenőrizheti, hogy kitől származnak az Ügyfél által a Banknak küldött Üzenetek.

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.

A Szolgáltatásokhoz és/vagy kapcsolódási csatornákhoz való hozzáférést biztosító Hitelesítési módszerekre vonatkozóan a CitiDirect Login Help (bejelentkezési tudnivalók) weboldalon található részletesebb felvilágosítás. Az Ügyfélnek mindig lehetősége van választani a rendelkezésre álló Hitelesítési módszerek közül. A Bank a szolgáltatások és/vagy kapcsolódási csatornák telepítése során beállíthat alapértelmezett Hitelesítési módszert, amelyet az Ügyfél bármikor módosíthat egy másik rendelkezésre álló Hitelesítési módszerre.

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

A szolgáltatásokhoz vagy kapcsolódási csatornákhoz való hozzáférés céljából az alábbi Hitelesítési módszerek állnak rendelkezésre:

CitiDirect Authentication Methods ***CitiDirect Hitelesítési módszerek***	
Biometrics *Biometrikus azonosítás*	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. *Olyan digitális azonosítási eljárás, amely a Felhasználó egyedi fizikai jellegeit felhasználva (mint pl. ujjlenyomat, arcfelismerés), a Felhasználó mobileszközébe beépített biometrikus technológia és kriptográfiai technikák segítségével biztosít belépést a CitiDirect-be. Ezen Hitelesítési mód esetén a fizikai tulajdonságokra vonatkozó adatok nem kerülnek továbbításra a Bank felé.*
Mobile Token (non-application based) *Mobiltoken* *(nem alkalmazásalapú)*	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. *Digitális, nem alkalmazás-alapú mobil hitelesítési módszer (pl. Mobil Token (nem alkalmazáshoz kötött)), amely kriptográfiai kulcsokat és biometrikus hitelesítést (például ujjlenyomatot és arcfelismerést) használ, hogy a felhasználó mobilböngészőjén keresztül összekapcsolja a felhasználó mobileszközét a CitiDirect fiókjával. Amikor a felhasználó ezt a hitelesítési módszert választja, fizikai tulajdonságokra vonatkozó adatok nem kerülnek továbbításra a Bank részére. Ez a módszer azáltal teszi lehetővé a többfaktoros hitelesítést, hogy a felhasználó személyazonosságát a regisztrált mobileszközével igazolja.*
Challenge Response Token *Hívó- és válaszkód Token*	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. *Mely lehet (i) egy mobil applikáció-alapú szoftver (pl. MobilePASS) vagy (ii) egy fizikai eszköz (pl. SafeWord kártya, Vasco), melynek segítségével minden alkalommal egy dinamikus, belépésenként változó jelszó generálódik egy PIN kóddal (pl. 4 számjegyű PIN) történő azonosítás után. A CitiDirect-be történő belépés alkalmával a rendszer létrehoz egy hívó kódot („challenge"), melyre az eszközzel (Token) generált válasz kód („response") beírásával biztosított a rendszerhez való hozzáférés. Ez a Hitelesítési módszer biztonságos jelszóval kombinálva többlépcsős azonosítást tesz lehetővé.*
One-Time Password Token *Egyszerhasználatos jelszó Token*	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. *Ami lehet (i) egy mobil applikáció-alapú szoftver (pl. MobilePASS) vagy (ii) egy fizikai eszköz (pl. SafeWord kártya, Vasco), melynek segítségével egy dinamikus, belépésenként változó jelszó generálódik egy PIN kóddal (pl. 4 számjegyű PIN) történő azonosítás után. A rendszerhozzáférés a jelszó bevitelével biztosított.*

CitiDirect Authentication Methods ***CitiDirect Hitelesítési módszerek***	
Secure Password *Biztonsági jelszó*	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. *A Felhasználó a biztonsági jelszava megadásával fér hozzá a rendszerhez. A biztonsági jelszó jellemzően korlátozza a Felhasználó rendszerjogosultságait, pl. csak bizonyos információk láthatók a Felhasználó számára. Ez a Hitelesítési módszer Hívó- és válaszkód Tokennel kombinálva többlépcsős hitelesítést tesz lehetővé.*
SMS One-Time Code *Egyszeri SMS jelszó*	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. *A Felhasználók részére a dinamikus, belépésenként változó jelszó SMS útján érkezik. A felhasználó ezt a belépésenként változó jelszót és a biztonsági jelszavát beírva tud belépni a rendszerbe.*
Voice One-Time Code *Egyszeri belépőkód hanghívással*	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. *A Felhasználó rögzített hanghíváson keresztül egy egyszer használatos jelszót kap. Ezt követően a Felhasználó az egyszer használatos jelszó és a biztonsági jelszó megadásával léphet be a rendszerbe.*
Digital Certificates *Digitális tanúsítványok*	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. *A hitelesítésre egy jóváhagyott tanúsító hatóság által kiadott digitális tanúsítvány szolgál. A digitális tanúsítványokat hitelesítés céljából egyedi felhasználóknak ("Személyes tanúsítványok") vagy vállalati jogi személyeknek ("Vállalati pecsétek") állítják ki. Az Ügyfél felelőssége, hogy a hatályos jogszabályoknak megfelelően ellenőrizze az Ügyfél nevében eljáró, Személyes tanúsítvánnyal rendelkező összes felhasználó személyazonosságát.* *A Bank által bármely nyilvános internetkapcsolaton keresztül fogadott kommunikációval szemben, vagy egyéb, nem biztonságos internetkapcsolat esetén elvárt, hogy a Bank és az Ügyfél között a digitális tanúsítványok használatával létrejöhessen egy biztonságos, titkosított csatorna, a küldött és fogadott adatok védelme érdekében.*

CitiConnect for Files Authentication Methods *CitiConnect for Files Hitelesítési módszerek*	
Digital Certificates *Digitális tanúsítványok*	See description above. *Lásd a fenti tájékoztatót.*

CitiConnect for Files Authentication Methods *CitiConnect for Files Hitelesítési módszerek*	
IP Address Whitelist When Using CitiConnect *IP-cím engedélyezési lista CitiConnect használatakor*	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. *A Bank bizonyos internetes kommunikációi, például egy virtuális magánhálózaton (VPN) keresztül is támaszkodhatnak arra, hogy a felek előre megbeszélt IP-címek használatával cseréljenek információkat. A Bank kizárólag az Ügyfél által megjelölt IP címről származó Üzeneteket fogad el (fordított esetben is igaz), továbbá a Bank kizárólag az Ügyfél által megjelölt IP címre küld Üzeneteket (fordított esetben is igaz). Alkalmazása a fent ismertetett Digitális Tanúsítványra épülő módszerrel együtt történik.*

CitiConnect API Authentication Methods ***CitiConnect API Hitelesítési módszerek***	
Digital Certificates *Digitális tanúsítványok*	See description above. *Lásd a fenti tájékoztatót*
IP Address Whitelist When Using CitiConnect *IP-cím engedélyezési lista CitiConnect használatakor*	See description above. *Lásd a fenti tájékoztatót.*

CitiConnect for SWIFT Authentication Methods ***CitiConnect for SWIFT Hitelesítési módszerek***	
Digital Certificates *Digitális tanúsítványok*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Lásd a fenti tájékoztatót. Együtt alkalmazható az alább ismertetett SWIFT Hitelesítési módszerrel.*

CitiConnect for SWIFT Authentication Methods *CitiConnect for SWIFT Hitelesítési módszerek*	
SWIFT Authentication *SWIFT hitelesítés*	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. *A Bank és az Ügyfél között a SWIFT hálózaton keresztül történő üzenetváltás – ideértve többek között a számlainformációkat, átutalási megbízásokat, valamint az ilyen megbízások módosítására vagy törlésére vonatkozó utasításokat – melyek vagy a SWIFT Általános Szerződési Feltételeit és a SWIFT FIN Szolgáltatási Leírását korlátozás nélkül tartalmazó (időről időre kiegészített vagy módosított) szerződéses dokumentációjában-, vagy a SWIFT által esetlegesen egyéb módon meghatározott eljárásokkal hitelesíthetők. A Bank nem köteles a SWIFT eljárásain kívül mindent megtenni az üzenet feladójának és hitelességének megállapítása érdekében.* *A Bank nem vállal felelősséget a SWIFT rendszer hibáiért és késedelmeiért. Az Ügyfél köteles a SWIFT által előírt és meghatározott formátumban és jellemzőknek megfelelően továbbítani a Banknak szánt üzeneteit.* *A SWIFT rendszeren keresztül küldött vagy fogadott kommunikációkra a hatályos SWIFT szabályok és rendeletek vonatkoznak, ideértve a tagsággal kapcsolatos szabályokat is. Az Ügyfél felelős a SWIFT üzenetküldési szabványok megismeréséért és az annak való megfelelésért.*

SWIFT Authentication Method ***SWIFT Hitelesítési Szabvány***	
SWIFT Authentication (Direct Connection for Financial Institutions) *SWIFT hitelesítés (közvetlen kapcsolat a pénzintézetek számára)* *keuangan)*	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. *A Bank és az Ügyfél között a SWIFT hálózaton keresztül történő üzenetváltás – ideértve többek között a számlainformációkat, átutalási megbízások, valamint az ilyen megbízások módosítására vagy törlésére vonatkozó utasításokat – melyek vagy a SWIFT Általános Szerződési Feltételeit és a SWIFT FIN Szolgáltatási Leírását korlátozás nélkül tartalmazó (időről időre kiegészített vagy módosított) szerződéses dokumentációjában-, vagy a SWIFT által esetlegesen egyéb módon meghatározott eljárásokkal hitelesíthetők. A Bank nem köteles a SWIFT eljárásain kívül mindent megtenni az üzenet feladójának és hitelességének megállapítása érdekében.* *A Bank nem vállal felelősséget a SWIFT rendszer hibáiért és késedelmeiért. Az Ügyfél köteles a SWIFT által előírt és meghatározott formátumban és jellemzőknek megfelelően továbbítani a Banknak szánt üzeneteit.* *A SWIFT rendszeren keresztül küldött vagy fogadott kommunikációkra a hatályos SWIFT szabályok és rendeletek vonatkoznak, ideértve a tagsággal kapcsolatos szabályokat is. Az Ügyfél felelős a SWIFT üzenetküldési szabványok megismeréséért és az annak való megfelelésért.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Digitális/Elektronikus aláírásra épülő Hitelesítési módszerek elektronikus dokumentumok benyújtásához***	
Digital Signature *Digitális aláírás*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Az elektronikus aláírások azon válfaja, amely digitális tanúsítványok segítségével ellenőrzi egy aláírás, üzenet, szoftver vagy digitális dokumentum hitelességét és integritását.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Digitális/Elektronikus aláírásra épülő Hitelesítési módszerek elektronikus dokumentumok benyújtásához***	
Electronic Signature *Elektronikus aláírás*	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. *Szerződéshez vagy egyéb okmányhoz csatolt olyan elektronikus jelzés, amely az aláíró fél által a dokumentum aláírása céljából alkalmazott, egyedi jelzés. Elektronikus aláírás létrehozható szavak, betűk, számjegyek, jelzések, weboldalon alkalmazott egérkattintás, telefax vagy fizikai formában készült szkennelt dokumentum feltöltése, érintőképernyő érintése, illetve bármely feltétel elektronikus úton történő elfogadása formájában. A használója kizárólagos hatáskörében létrehozott digitális aláírás logikailag egy adatokat tartalmazó üzenethez kapcsolódik, vagy a rendszer ilyenhez rendeli hozzá; és alkalmasnak kell lennie az üzenetben történő adatküldéshez hozzájáruló személy azonosítására, és tanúsítania kell, hogy az illető megadta hozzájárulását. Az ilyen Elektronikus aláírást a Bank elektronikus csatornáin, az ismertetett és hozzá tartozó Hitelesítési módszereknek megfelelően kell benyújtani a Bankhoz.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Manuálisan kezdeményezett átutalási megbízások – Manually Initiated Funds Transfer („MIFT") Hitelesítési módszerek***	
MIFT Authentication *MIFT hitelesítés*	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. *A Manuálisan kezdeményezett átutalási megbízások (Manually Initiated Funds Transfer, „MIFT") – és a korábbi Manuálisan kezdeményezett megbízások módosítása, visszavonása, törlése – telefaxon vagy levélben küldhető el, illetve feltölthető a CitiDirect rendszerbe. Egyes országokban nem érhető el az összes megbízástípus. A kezdeményezők az Ügyfél által kijelölt személyek, akiket az Ügyfél felhatalmazott arra, hogy a megfelelő korlátozások mellett ügyletekre adjanak megbízásokat. A jóváhagyók az Ügyfél által kijelölt olyan személyek, akiket a Bank saját belátása szerint felhívhat, hogy a Manuális úton kezdeményezett átutalási megbízások megerősítését kérje.* *Egyes országokban mobiltelefonszám nem adható meg ellenőrzési célú visszahíváshoz. Az adott országra vonatkozó Termékspecifikus Feltételek, a Globális Pénzforgalmi és Szolgáltatási Feltételek, valamint a Meghatalmazás Manuális Tranzakciók Kezelésére nyomtatvány vagy az Univerzális megbízási nyomtatvány részletesebb tájékoztatást nyújt erre vonatkozóan. Az MIFT módszert az Ügyfél szükségmegoldásként veheti igénybe olyan célra, hogy utasításokat közöljön a Bankkal.*

Mail, Fax, Email and Messenger Authentication Methods ***Posta, telefax, e-mail és Messenger mint Hitelesítési módszerek***	
Seal Image Verification *Bélyegző képe alapján végzett ellenőrzés*	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. *A telefaxon, postán, e-mailben vagy futárral beérkező Üzeneteket – a MIFT kérelmek kivételével – a Bank az Ügyféltől kapott meghatalmazásban vagy hasonló dokumentumban szereplő bélyegző képe alapján, kellő körültekintéssel ellenőrzi és állítja össze*
Signature Verification *Aláírás ellenőrzése*	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. *A telefaxon, postán, e-mailben vagy futárral beérkező Üzeneteken – a MIFT kérelmek kivételével – szereplő aláírásokat a Bank az Ügyféltől kapott meghatalmazásban vagy hasonló dokumentumban szereplő adatok alapján ellenőrzi.*
Secure PDF *Biztonságos PDF (secured mail)*	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. *A titkosított e-mailek egy kijelölt postafiókba PDF dokumentumként kerülnek, melyeket egy privát, biztonsági jelszó megadásával lehet megnyitni. Az üzenet maga és a csatolmány is titkosításra kerül. Az egyéni jelszó az első biztonságos üzenet megnyitása alkalmával adható meg.*
MTLS *MTLS*	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. *Mandatory Transport Layer Security (MTLS) biztonságos, privát e-mail kapcsolatot létesít a Bank és az Ügyfél között. Az interneten keresztül ezen a csatornán továbbított e-mailek a kapcsolat által létrehozott titkosított TLS csatornán kerülnek továbbításra.*

Phone Authentication Methods ***Telefonhíváshoz kapcsolódó Hitelesítési módszerek***	
PIN *PIN*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *A Bankot telefonon megkereső Ügyfelek felhasználóinak meg kell adniuk az erre a célra létrehozott PIN kódjukat hozzáférési jogosultságuk igazolása céljából.*
Verification Questions *A jogosultságot ellenőrző kérdések*	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. *A Bankot telefonon megkereső Ügyfelek felhasználóit a Bank ügyfélszolgálati munkatársa megkéri, hogy ellenőrző kérdésekre adott szóbeli válaszokkal igazolják hozzáférési jogosultságukat.*

The availability of Authentication Methods described above varies based on local markets.
A fentebb ismertetett Hitelesítési módszerek elérhetősége országonként eltérő lehet.

3. Customer Responsibilities
Az Ügyfél kötelezettségei

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.

Jogosult Felhasználók azonosítása: Az Ügyfél köteles ellenőrizni mindazok személyazonosságát, akik (i) az Ügyfél nevében egy adott vállalat szintjén az összes Szolgáltatás és kapcsolódási csatorna tekintetében a Számlá(k)ra vonatkozóan eljárnak, továbbá (ii) akiket az Ügyfél jogszabályi előírásoknak megfelelően felhatalmazott arra, hogy az Ügyfél Számlája vonatkozásában eljárjanak.

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.

Az Ügyfél felelős kijelölni és ellenőrizni az Ügyfél és/vagy felhasználói számára kijelölt tranzakciós limiteket, és biztosítani, hogy ezek a limitek (a) ne haladják meg az Ügyfél belső szabályzataiban és egyéb, jogköröket meghatározó, valamint alapító dokumentumaiban, mint például az Ügyfél igazgatósági határozatai, banki felhatalmazások, egyéb Ügyvédi meghatalmazásokban vagy ezeknek megfelelő dokumentumokban előírt limiteket, továbbá (b) biztosítani, hogy ezek összhangban legyenek minden kapcsolódási csatornára kiadott felhasználói jogosultságokkal.

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.

Egyes országok hatóságai megkövetelhetik, hogy a Bank csak akkor biztosítson hozzáférést bizonyos funkciókhoz az ezeket használni kívánók számára, ha előbb a pénzmosás megelőzésére vonatkozó jogszabályi követelményeknek megfelelően ellenőrizte személyazonosságukat (és azonosító adataik megfelelőségét). További felvilágosításért forduljon ügyfélszolgálati kapcsolattartójához, vagy látogasson el a CitiDirect weboldalára.

3.4 Safeguarding of Authentication Methods
A Hitelesítési módszerek biztonsága

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.

Az Ügyfél köteles a lehető legnagyobb gondossággal és körültekintés mellett biztosítani a Hitelesítési módszerek és Hitelesítési adatok megfelelő védelmét, továbbá azt, hogy a Hitelesítési adatokhoz kizárólag az Ügyfélnél erre felhatalmazott személyek férhessenek hozzá.

Harmadik fél által küldött Üzenetek: Ha az Ügyfél Hitelesítési adatot használ az Üzenetek azonosítása és hitelesítése érdekében, hogy biztosítsa, az Üzenetek tőle, mint jogi személytől származnak, akkor az Ügyfél felelős azért, hogy a Bank számára történő Üzenetküldés során teljes körű ellenőrzést gyakoroljon az ilyen jellegű Hitelesítő adatok felett, ideértve azokat az eseteket is, amikor az Üzenetek továbbítása az Ügyfél megbízásából harmadik fél által üzemeltetett alkalmazásokon és/vagy rendszereken keresztül történik. A Bank (a) az Ügyféltől származó Üzenetnek tekint minden olyan, a Bank által elektronikus kapcsolattartásra használt csatornán keresztül érkezett Üzenetet, amely esetében a jelen Biztonsági eljárások alapján kielégítően igazolható, hogy az Ügyféltől származik, továbbá (b) jogosult az Ügyféltől a jelen Biztonsági eljárásoknak megfelelően kapott Üzenetekben foglaltak szerint eljárni.

4. Data Integrity and Secured Communications
Adatintegritás és biztonságos üzenetváltás

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.

Az Ügyfél tudomásul veszi, hogy az általa interneten, postai úton, e-mailben és/vagy telefaxon küldött adatok és a Bankkal egyéb módon váltott üzenetek (i) nem feltétlenül minősülnek biztonságos kommunikációs és kézbesítési rendszernek, és (ii) nem állnak a Bank ellenőrzése, irányítása alatt. Az Ügyfél tudomásul veszi továbbá, hogy amennyiben az Ügyfél felhasználói jogosultak hozzáférni a Citi rendszerein kívüli nyílt bankolásos rendszerhez és/vagy hasonló harmadik fél platformjaihoz, az Ügyfél adatai továbbításra kerülhetnek az ilyen, a Bank ellenőrzésén kívül eső harmadik fél platformjain keresztül.

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.

A Bank (saját megítélése szerint) a jelenleg piacvezetőnek számító titkosítási módszereket alkalmazza annak érdekében, hogy biztosítsa az információk bizalmas kezelését, és megakadályozza, hogy ezek az elektronikus továbbítás közben módosuljanak.

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.

Ha az Ügyfél gyanítja vagy tudomást szerez arról, hogy a Bank szolgáltatásaival, kapcsolódási csatornáival vagy Hitelesítési módszereivel kapcsolatban technikai hiba lépett fel vagy esetlegesen csalárd hozzáférés vagy használat történhetett bármely személy (függetlenül attól, hogy az a személy jogosult vagy sem azok használatára) által, az Ügyfél köteles erről haladéktalanul értesíteni a Bankot. Felhatalmazott személy általi illetéktelen, vagy feltehetően csalás útján történő hozzáférés vagy használat esetén az Ügyfélnek haladéktalanul intézkednie kell annak érdekében, hogy megakadályozza a Bank szolgáltatásaihoz vagy kapcsolódási csatornáihoz történő hozzáférést, illetve azok használatát az illető részéről.

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.

Ha az Ügyfél (a Banktól vagy harmadik féltől származó) fájlformázó vagy titkosító szoftvert használ az Ügyfél adatainak és megbízásainak formázására és felismerésére, és a Banktól kapott Üzenetekben foglaltak szerint jár el, akkor az Ügyfél az ilyen szoftvert kizárólag arra a célra használhatja, amely célból a szoftvert telepítették.

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.

Az Ügyfél tudomásul veszi és elfogadja, hogy a Bank felfüggesztheti vagy letilthatja azon Felhasználók hozzáférését a Hitelesítési adatok megadásával elérhető Szolgáltatásokhoz, ha (i) fennáll a Hitelesítési adatokkal való visszaélés vagy azok illetéktelen használatának gyanúja, és/vagy (ii) ha a Szolgáltatások, valamint a Hitelesítési adatok védelme ezt indokolja.

5. Security Manager and Related Functions
A Rendszeradminisztrátor és az ehhez kapcsolódó funkciók

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:

A CitiDirect és a CitiConnect rendszerben elérhető alkalmazásokhoz (az alább ismertetett Egyéni Tanúsítványok kivételével), a Bank elvárja az Ügyféltől, hogy úgynevezett „Rendszeradminisztrátor" funkciót hozzon létre. A Rendszeradminisztrátorok feladatai:

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 Felhasználók (magukat a Rendszeradminisztrátorokat is beleértve) hozzáféréseinek és jogosultságainak létrehozása és karbantartása, amely például az alábbi tevékenységeket foglalja magában: (a) felhasználói profilok (a Rendszeradminisztrátori profilokat is ideértve), valamint jogosultságok létrehozása, törlése vagy módosítása (Figyelem! A felhasználó nevének egyeznie kell az igazolásul használt személyazonosító okmányon szereplő névvel) (b) olyan hozzáférési profilok létrehozása, amelyek meghatározzák, hogy az egyes felhasználók milyen funkciókhoz és adatokhoz férhetnek hozzá, (c) a felhasználók bejelentkezési adatainak aktiválása és érvénytelenítése; és (d) tranzakciós limitek beállítása (Figyelem! A Bank nem kíséri figyelemmel és nem ellenőrzi a beállított tranzakciós értékhatárokat; a limitek figyelése, és annak biztosítása, hogy azok összhangban legyenek az Ügyfél belső szabályzataival és előírásaival, ideértve többek között az Ügyfél igazgatósága által bevezetett- vagy azokkal egyenértékű szabályokat, az Ügyfél feladata);

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;

Bejegyzések létrehozása és módosítása az Ügyfél által karbantartott könyvtárakban (pl. előre rögzített átutalás-minták és kedvezményezettekre vonatkozó adatokat tartalmazó könyvtárak), és más felhasználók számára jogosultság biztosítása ugyanezen műveletekre vonatkozóan;

5.3 Modifying payment authorization flows;

Az átutalások engedélyezési folyamatainak módosítása;

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

Dinamikus, belépésenként változó jelszavak, valamint a rendszerbe való belépéshez szükséges egyéb bejelentkezési adatok és jelszavak kiosztása az Ügyfél felhasználóinak;

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

A Bank értesítése abban az esetben, ha okkal gyanítható, hogy az adatbiztonság veszélybe került; és

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

Digitális tanúsítványok kezelése és beszerzése, valamint további felhasználók felhatalmazása erre.

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.

Figyelem: A Rendszeradminisztrátorok feladat- és felelősségi köre a jogszabályi előírásoktól és/vagy a rendelkezésre álló lehetőségektől függően egyes országokban eltérő lehet, vagy akár az ilyen funkció létrehozása sem lehetséges. Ezen országokban előfordulhat, hogy a Bank további dokumentumokat vagy egyéb adatokat kér be az Ügyféltől annak érdekében, hogy a Bank láthassa el a szóban forgó Rendszeradminisztrátori feladatokat az Ügyfél számára.

6. Use of CitiDirect and CitiConnect by Security Managers
A CitiDirect és a CitiConnect használata a Rendszeradminisztrátorok által

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.

A Bank előírása szerint két (2) külön személy rögzíthet és engedélyezhet megbízásokat; ezért legalább két Rendszeradminisztrátorra van szükség. Bármely két, együttesen eljáró Rendszeradminisztrátor jogosult bármely Rendszeradminisztrátor funkciót illetően, vagy az Üzenetváltás elősegítésével összefüggésben utasításokat megadni és/vagy megerősítéseket tenni a kapcsolatot biztosító csatornákon keresztül. Két Rendszeradminisztrátor által jóváhagyott bármely utasítást a Bank az Ügyfél által küldött utasításnak tekint és végrehajtja az abban foglaltakat. A biztonságos működés érdekében a Bank javasolja legalább három Rendszeradminisztrátor kinevezését. Az Ügyfél az Elektronikus csatorna - igénylőlapon (Channels Onboarding Form) tudja kijelölni a Rendszeradminisztrátorait. Az Ügyfél Rendszeradminisztrátora harmadik fél (például az Ügyfél kapcsolt vállalata) Rendszeradminisztrátoraként is tevékenykedhet, és gyakorolhatja az ezzel kapcsolatos jogait (ideértve felhasználók beállítását az illető harmadik fél Számlájához (Számláihoz)) – minden további meghatalmazás nélkül –, ha a harmadik fél a Felhatalmazás Univerzális Hozzáférésre (UAA) elnevezésű igénylőlapon (vagy a Bank számára elfogadható egyéb felhatalmazáson) hozzáférési jogosultságot biztosít Számlájához (Számláihoz) a harmadik fél számára. Ez a jogosultság kizárólag az adott felhatalmazás tárgyát képező Számlá(k) vonatkozásában érvényes.

7. Use of CitiDirect by Security Officers (For Personal Certificates only) *A CitiDirect használata a Biztonsági munkatársak részéről (kizárólag Egyéni Tanúsítványok esetén)*

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.

A Bank előírja, hogy a magánszemélyekhez tartozó digitális tanúsítványokat („Egyéni Tanúsítványok") két (2) külön személy kezelje. Ezért a felhasználók számára a kapcsolódási csatornákon keresztül történő Üzenetváltások hitelesítéséhez és engedélyezéséhez szükséges Egyéni Tanúsítványt csak két Biztonsági munkatárs adhat ki vagy vonhat vissza. A biztonságos működés érdekében a Bank javasolja legalább három Biztonsági munkatárs kinevezését. Két Biztonsági munkatárs által jóváhagyott bármely utasítást a Bank az Ügyfél által küldött utasításnak tekint és végrehajtja az abban foglaltakat.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions