



Podręcznik dotyczący usług świadczonych
przez Bank Handlowy w Warszawie S.A.

Polska

Spis treści

I. Wprowadzenie	3
II. Obsługa płatności	4
A. Rodzaje usług płatniczych świadczonych przez Bank w Polsce	4
B. Realizacja płatności	4
C. Polecenie zapłaty (Klient jako płatnik)	5
D. Wypłaty gotówkowe	7
III. Obsługa należności	11
A. Otrzymywanie płatności	11
B. Polecenie zapłaty (Klient jako wierzyciel)	11
C. Wpłaty w Banku	12
D. Wpłaty gotówkowe	13
E. SpeedCollect	16
F. ARMS (<i>Account Receivables Matching Service</i>)	17
IV. Pozostałe kwestie	19
V. Formularze elektroniczne	21
VI. Skonsolidowane procedury bezpieczeństwa Bankowości Transakcyjnej	22
A. Role i obowiązki Administratora Systemu*	22
B. Metody Uwierzytelniania	24
C. Integralność Danych i Bezpieczna Komunikacja	27
VII. Podsumowanie	28

I. Wprowadzenie

Dziękujemy za wybór Bankowości Transakcyjnej (*Treasury and Trade Solutions*, TTS) Banku Handlowego w Warszawie S.A. („Bank”) na potrzeby zarządzania środkami finansowymi w Państwie firmie. Niniejszy Podręcznik dotyczący usług świadczonych przez Bank Handlowy w Warszawie S.A. ma służyć klientom jako podręcznik przedstawiający szczegółowe informacje o dostępnych dla nich usługach.

Z niniejszym podręcznikiem należy się zapoznawać łącznie z dokumentami Lokalne Warunki Prowadzenia Rachunków i Świadczenia Usług obowiązujące w Banku Handlowym w Warszawie S.A. („Warunki Lokalne”), Ogólnymi Warunkami Prowadzenia Rachunków i Świadczenia Usług obowiązującymi w Banku Handlowym w Warszawie S.A. („Ogólne Warunki”), Zasadami Dotyczącymi Poufności i Ochrony Danych Osobowych („Zasady”), Wymogami Regulacyjnymi, Zapewnieniami i Oświadczeniami obowiązującymi w Banku Handlowym w Warszawie S.A. („Wymogi”), taryfą opłat i prowizji Banku oraz wnioskami o uruchomienie poszczególnych produktów. Niniejszy przewodnik może być w dowolnej chwili aktualizowany przez Bank za powiadomieniem Klienta za pośrednictwem oficjalnych kanałów komunikacji Banku.

II. Obsługa płatności

A. Rodzaje usług płatniczych świadczonych przez Bank w Polsce

- Przelewy wewnętrzne: przelewy między rachunkami prowadzonymi w Banku
- Przelewy krajowe: przelewy realizowane przez system Krajowej Izby Rozliczeniowej S.A. (tj. system KIR) i SORBNET (tj. system NBP obsługujący zarówno przelewy o wysokiej wartości, jak i o niskiej wartości), kierowane na rachunek prowadzony przez inny bank w Polsce
- Przelewy wysokokwotowe (*Real-Time Gross Settlement, RTGS*) - przelewy realizowane przez NBP (SORBNET2): system przelewów o wysokiej wartości oparty na bieżącym rozrachunku poszczególnych zleceń płatniczych
- Jednolity obszar płatności w euro (*Single European Payments Area, SEPA*): mechanizm rozliczeń płatności masowych EUR, obejmujący zarówno opartą o zgodę usługę polecenia zapłaty, jak i usługę polecenia przelewu.
- Płatności natychmiastowe (*Express Elixir*): krajowe przelewy elektroniczne realizowane w czasie rzeczywistym, stosowane do przekazywania środków pieniężnych z rachunku w Banku na rachunek w innym Banku za pośrednictwem KIR. Maksymalna kwota transakcji wynosi 100 000 PLN.
- Polecenie zapłaty: sposób pobierania kwot pieniężnych należnych od płatnika, w którym beneficjent inicjuje transakcję, którą przetwarza bank płatnika na jego rachunku. Polecenie zapłaty, które zawsze wymaga zgody płatnika, jest zazwyczaj stosowane w przypadku powtarzających się płatności, takich jak rachunki za media, w których kwoty płatności różnią się między sobą.
- Przelewy transgraniczne: umożliwiają klientom Banku wykonywanie wychodzących międzynarodowych przelewów telegraficznych w wielu walutach.

B. Realizacja płatności

1. Klient przesyła do Banku dyspozycję polecenia przelewu, sformatowaną zgodnie ze standardami rynkowymi i wytycznymi podanymi podczas wdrażania usługi, z wykorzystaniem:
 - kanałów bankowości elektronicznej Banku, w tym CitiDirect BE[®] i CitiConnect[®], lub
 - interfejsu SWIFT
 - ręcznie inicjowanego przelewu (*Manually Initiated Funds Transfer, „MIFT”*)
2. Dyspozycja polecenia przelewu jest zautoryzowana przez Klienta, jeżeli:
 - w przypadku kanału bankowości elektronicznej – transakcje zostały wprowadzone zgodnie ze Skonsolidowanymi procedurami bezpieczeństwa Bankowości Transakcyjnej i przekazane do Banku przez opisany tam kanał dostępu,

- w przypadku MIFT – dyspozycja polecenia przelewu została podpisana przez osoby upoważnione zgodnie z kartą wzorów podpisów i uznaje się ją za otrzymaną, jeśli została dostarczona do placówki Banku akceptującej takie dyspozycje,
- w przypadku SWIFT – Klient wprowadził dyspozycję polecenia przelewu do systemu SWIFT w taki sposób, by Bank mógł zapoznać się z jej treścią.

Bank może wprowadzić procedury zabezpieczające dotyczące każdej z form składania dyspozycji przez Klienta. Bank może potwierdzić telefonicznie z osobami wskazanymi przez Klienta dyspozycje skutkujących obciążeniem Rachunku .

Bank nie zrealizuje dyspozycji w przypadku:

- braku uzyskania potwierdzenia przez telefon lub mimo uzyskania potwierdzenia,
 - jeśli w opinii Banku potwierdzenie takie nie jest tożsame z treścią dyspozycji przesłanej do Banku.
3. Bank przekazuje dyspozycję do właściwego systemu płatniczego w celu dalszego przetwarzania.
 4. System płatniczy przekazuje dyspozycję do banku beneficjenta w oparciu o lokalnie zdefiniowany cykl rozliczeniowy.
 5. Bank beneficjenta uznaje rachunek beneficjenta.

C. Polecenie zapłaty (Klient jako płatnik)

Bank – jako bank Klienta – obsługuje dyspozycje polecenia zapłaty otrzymywane od innych współpracujących instytucji finansowych. W Polsce Bank obsługuje płatności w drodze krajowego polecenia zapłaty w PLN i polecenia zapłaty SEPA (w trybie CORE i B2B).

Zgoda na polecenie zapłaty

Klient zgadza się na obciążanie jego rachunku poprzez podpisanie zgody na polecenie zapłaty. Zgody muszą zawierać niepowtarzalny identyfikator Klienta, niepowtarzalny identyfikator odbiorcy i niepowtarzalny identyfikator płatności. Zgody muszą być przekazywane odbiorcy lub Bankowi w formie pisemnej lub w innej wcześniej uzgodnionej formie. Zgody na polecenie zapłaty SEPA (w trybie CORE) muszą być przekazywane wyłącznie odbiorcy, a w trybie B2B zarówno Bankowi, jak i odbiorcy.

Klient może w dowolnym czasie odwołać zgodę na krajowe polecenie zapłaty lub polecenie zapłaty SEPA B2B, składając dyspozycję zawierającą następujące elementy:

- numer rachunku, imię i nazwisko oraz podpis Klienta;
- imię i nazwisko (nazwę) odbiorcy;
- niepowtarzalny identyfikator odbiorcy;
- niepowtarzalny identyfikator transakcji określony przez stosunek prawny pomiędzy Klientem a odbiorcą.

Bank zakończy wykonywanie usługi polecenia zapłaty w ciągu 3 dni roboczych od otrzymania dyspozycji odwołania.

Klient nie może odwołać zgody na polecenie zapłaty SEPA w trybie CORE.

Zwrot środków w trybie polecenia zapłaty

W ciągu 5 dni roboczych od dnia, w którym obciążono rachunek, Klient może złożyć Bankowi dyspozycję zwrotu środków, którymi uprzednio obciążono jego rachunek w ramach usługi polecenia zapłaty. Dyspozycje zwrotu mogą być składane w formie pisemnej na adres podany na stronach internetowych Banku lub przez CitiDirect BE®.

Dyspozycje zwrotu powinny zawierać następujące elementy:

- numer rachunku Klienta;
- niepowtarzalny identyfikator odbiorcy;
- niepowtarzalny identyfikator transakcji określony przez stosunek prawny pomiędzy Klientem a odbiorcą;
- kwotę, jaką obciążono rachunek Klienta;
- dzień, w którym obciążono rachunek Klienta.

Jeżeli Klient skorzystał z usługi polecenia zapłaty SEPA w trybie CORE, może złożyć dyspozycję zwrotu środków, w ciągu ośmiu tygodni od dnia, w którym obciążono jego rachunek. Dyspozycje zwrotu środków mogą być składane wyłącznie w formie pisemnej. Klient nie może złożyć dyspozycji zwrotu środków w przypadku skorzystania z usługi polecenia zapłaty SEPA w trybie B2B.

Odwołanie planowanych obciążeń w trybie polecenia zapłaty

Klient może złożyć dyspozycję odwołania płatności wykonywanej w ramach usługi polecenia zapłaty najpóźniej do końca dnia roboczego poprzedzającego uzgodniony dzień, w którym rachunek Klienta ma być obciążony. Dyspozycje takie mogą być składane w formie pisemnej na adres podany na stronach internetowych Banku lub przez CitiDirect BE®.

Dyspozycje odwołania płatności powinny zawierać następujące elementy:

- numer rachunku i niepowtarzalny identyfikator odbiorcy;
- niepowtarzalny identyfikator transakcji określony przez stosunek prawny pomiędzy Klientem a odbiorcą;
- dzień, w którym rachunek Klienta ma być obciążony.

Klient nie może złożyć dyspozycji anulowania płatności w przypadku polecenia zapłaty SEPA, w trybie B2B ani w trybie CORE.

Odmowa realizacji polecenia zapłaty

Bank może odmówić wykonania dyspozycji obciążenia rachunku Klienta (płatnika) w ramach usługi polecenia zapłaty w następujących sytuacjach:

- środki pieniężne na rachunku Klienta są niewystarczające do pokrycia pełnej kwoty transakcji polecenia zapłaty;
- rachunek Klienta jest zamknięty;

- nie została wydana zgoda na polecenie zapłaty;
- zgoda została odwołana;
- dane podane w zgodzie na polecenie zapłaty nie zgadzają się z danymi zawartymi w dyspozycji płatności zainicjowanej przez odbiorcę;
- została złożona dyspozycja anulowania płatności.

Proces płatności w ramach polecenia zapłaty

1. Przed dokonaniem płatności Bank porównuje otrzymaną transakcję ze zgodą Klienta na polecenie zapłaty.
2. Jeżeli płatność w ramach polecenia zapłaty jest zgodna ze zgodą Klienta na polecenie zapłaty, Bank przetwarza dyspozycję płatności i obciąża rachunek Klienta.
3. Jeżeli środki pieniężne na rachunku Klienta są niewystarczające, Bank nie przetwarza płatności w ramach polecenia zapłaty i odsyła do systemu płatności w ramach poleceń zapłaty lub do banku partnerskiego informację o nieudanej realizacji obciążenia.

Bank anuluje każdą pomyłkowo wykonaną operację i obciąża lub uznaje odpowiedni rachunek.

D. Wypłaty gotówkowe

Bank oferuje wypłaty gotówkowe jako wypłaty gotówki w formie otwartej (gotówka liczona w obecności Klienta) lub w formie zamkniętej (pakiety środków pieniężnych w bezpiecznych kopertach przygotowanych bez udziału Klienta) za pośrednictwem wyspecjalizowanych dostawców usług.

Wypłaty gotówki w formie otwartej mogą być dokonywane:

- w placówkach Banku, w walucie krajowej (w bilonie i banknotach) lub obcej (w banknotach). Lista walut obcych akceptowanych przez Bank jest dostępna na stronie internetowej Banku. Klienci mogą inicjować taką wypłatę na trzy sposoby:
 - złożenie podpisanego czeku wystawionego przez Bank;
 - złożenie pisemnej dyspozycji wypłaty podpisanej przez upoważnione osoby

Transakcje te są uznawane za zautoryzowane, gdy są dostarczone do Banku z odpowiednimi podpisami.

 - przesłanie pliku za pośrednictwem CitiDirect BE[®] zgodnie ze strukturą szablonu Banku (limit jednorazowej wypłaty na osobę to 5000 PLN lub równowartość tej kwoty w walucie obcej). Wypłaty na podstawie przesłanego pliku mogą być zrealizowane wyłącznie w ciągu trzech miesięcy od daty otrzymania pliku przez Bank.

Transakcje te są uznawane za zautoryzowane, gdy wykonane są przez Klienta zgodnie ze Skonsolidowanymi procedurami bezpieczeństwa Bankowości Transakcyjnej i przesłane do Banku za pośrednictwem CitiDirect BE[®].

- w urzędach pocztowych wymienionych na stronie internetowej spółki Poczta Polska S.A. (www.poczta-polska.pl), z wyjątkiem placówek oznaczonych jako agencje pocztowe; wypłaty realizowane wyłącznie w PLN.

Wypłaty gotówki w formie zamkniętej mogą być dokonywane przez jednostki liczące (sortownie) w walucie krajowej (bilon/banknoty) lub obcej (tylko banknoty).

Wypłaty na poczcie - proces

1. Klient wypełnia Wniosek o uruchomienie produktu i wskazuje rachunek, który będzie wykorzystywany do wypłat gotówki.
2. Klient wypełnia zlecenie wypłaty gotówkowej z tytułem płatności uzupełnionym zgodnie z wytycznymi Banku i przesyła je przez CitiDirect BE[®]. Transakcje te są uznawane za zautoryzowane, gdy wykonane są przez Klienta zgodnie ze Skonsolidowanymi procedurami bezpieczeństwa Bankowości Transakcyjnej i przesłane do Banku za pośrednictwem CitiDirect BE[®].

W przypadku wypłat przekraczających kwotę 30 000 PLN Klient wysyła email na adres: pze.wyciagibank@poczta-polska.pl oraz ekspres.pieniezny@citi.com

do godz. 12:00 na co najmniej cztery dni robocze przed wypłatą. Wiadomość musi zawierać:

- a. kwotę wypłaty
 - b. lokalizację pocztową, w tym numer i dokładny adres;
 - c. imię i nazwisko odbiorcy;
 - d. datę wypłaty gotówki.
3. Bank sprawdza rachunek Klienta i przekazuje środki na rachunek Poczty Polskiej. Zlecenia wypłaty z jakiegokolwiek rachunku Klienta innego niż wskazany we Wniosku o uruchomieniu produktu nie są realizowane. Zlecenie wypłaty jest nieodwołalne po obciążeniu rachunku Klienta.
 4. W dniu roboczym następującym po przekazaniu środków pieniężnych Klient otrzymuje email lub SMS od Poczty Polskiej z informacją, że środki pieniężne są już gotowe do wypłaty. Każde takie zawiadomienie zawiera numer identyfikacyjny transakcji (UIP).
 5. Wypłata będzie dostępna przez siedem dni roboczych od otrzymania numeru UIP w każdej wybranej placówce pocztowej wskazanej na stronach internetowych spółki Poczta Polska S.A.
 6. Odebranie wypłaty gotówki wymaga:
 - a. przedstawienia dokumentu tożsamości, który Klient wskazał w zleceniu wypłaty, oraz
 - b. numeru UIP. Utracone przez Klienta numery UIP można uzyskać, kontaktując się z CitiService.

7. Jeżeli wypłata nie może zostać dokonana ze względu na brak środków pieniężnych w danej placówce pocztowej, Klient zostaje skierowany do najbliższej placówki dysponującej wystarczającymi środkami.
8. Jeżeli wypłata gotówki nie zostanie dokonana w ciągu siedmiu dni, Poczta Polska przekazuje niepodjęte środki do Banku. Bank dokonuje zwrotu środków pieniężnych na rachunek Klienta najpóźniej do godz. 12:00 cztery dni robocze po ich otrzymaniu od Poczty Polskiej.

Proces wypłaty gotówki w formie zamkniętej

1. Klient przesyła formularz zlecenia wypłaty gotówkowej (zgodnie z szablonem udostępnionym przez Bank) przez CitiDirect BE[®] do godz. 12:00 na co najmniej dwa dni robocze przed datą wypłaty. Transakcje te są uznawane za zautoryzowane, gdy wykonane są przez Klienta zgodnie ze Skonsolidowanymi procedurami bezpieczeństwa Bankowości Transakcyjnej i przesłane do Banku za pośrednictwem CitiDirect BE[®]. W przypadku awarii CitiDirect BE[®] zlecenie wypłaty gotówkowej może zostać przesłane faksem na numer 22 690 14 95, a oryginał musi być dostarczony do Banku w dniu dokonywania wypłaty.
2. Monety powinny być zamawiane po 50 (rulony) lub 500 (woreczki). Bank dostarcza zamawiane nominały w miarę dostępności.
3. Klient odbierając gotówkę sprawdza pakiet i potwierdzenie doręczenia. Uszkodzone lub niewłaściwie zamknięte pakiety nie powinny być przyjmowane. Jeżeli numer pakietu nie odpowiada temu na potwierdzeniu doręczenia lub jeśli potwierdzenie doręczenia zawiera jakiegokolwiek poprawki lub skreślenia, dany pakiet nie powinien być przyjmowany. Podpisanie przez Klienta potwierdzenia doręczenia oznacza, że pakiet został uznany za nienaruszony.
4. Wyłącznym dowodem wartości wypłaty przekazanej Klientowi jest wyciąg bankowy.
5. Klient otwiera i przelicza zawartość pakietu lub pakietów w obecności co najmniej dwóch pracowników Klienta. Jeżeli kwota wskazana na zleceniu wypłaty różni się od kwoty przeliczonej przez Klienta, Klient musi w ciągu dwóch dni roboczych złożyć reklamację. Reklamacje muszą zawierać oryginalne opakowanie, kopię zbiorowej specyfikacji, opakowanie rulonu monet (jeżeli ma to zastosowanie) z podpisem i numerem osoby przygotowującej dany rulon i wszelkie pozostałe elementy podpisane przez osoby je przygotowujące.
6. Lokalizacje sortowni mogą ulegać zmianom. Bank zawiadamia Klienta o tym fakcie listownie lub elektronicznie a zmiany mają zastosowanie od dnia wskazanego w zawiadomieniu.

Elektroniczny przekaz pocztowy

1. Klient przesyła Zlecenie Przekazu przez CitiDirect BE[®]. Transakcje te są uznawane za zautoryzowane, gdy wykonane są przez Klienta zgodnie ze Skonsolidowanymi procedurami bezpieczeństwa Bankowości Transakcyjnej i przesłane do Banku za pośrednictwem CitiDirect BE[®].

2. Środki pieniężne, prowizja Poczty Polskiej oraz dane beneficjenta są przekazywane przez Bank ze wskazanego rachunku Klienta na rzecz Poczty Polskiej. Maksymalna kwota zlecenia wynosi 99 999,99 PLN. Doręczenie gotówki realizuje spółka Poczta Polska S.A.
3. W przypadku zmiany prowizji przez Poczta Polską Klient zostaje powiadomiony o tym fakcie pisemnie. Zmiany mają zastosowanie od dnia wskazanego w zawiadomieniu.
4. W przypadku braku środków na pokrycie prowizji Poczty Polskiej Bank wstrzymuje wykonywanie przekazu danego dnia i telefonicznie informuje o tym Klienta. W przypadku braku środków kolejnego dnia Bank dokonuje zwrotu środków na rachunek Klienta.
5. Gotówka jest doręczana pod adres wskazany w zleceniu w ciągu czterech dni roboczych od złożenia zlecenia przez Klienta. W przypadku gdy osoba doręczająca nie znajdzie beneficjenta pod wskazanym adresem, pracownik Poczty Polskiej zostawi awizo i ponowi próbę doręczenia gotówki w ciągu kolejnych siedmiu dni. W przypadku niepowodzenia drugiej próby doręczenia gotówki środki pieniężne są zwracane na rachunek Klienta wskazany we Wniosku o uruchomienie produktu, a Klient jest obciążany prowizją za zwrot.

III. Obsługa należności

A. Otrzymywanie płatności

1. Bank otrzymuje dyspozycję płatniczą poprzez system rozliczeniowy w oparciu o lokalnie zdefiniowany cykl rozliczeniowy.
2. Bank uznaje rachunek Klienta.

Wszelkie odrzucenia lub zwroty będą zwracane przez Bank na rachunek płatnika. Płatnikowi podawany jest powód zwrotu.

W przypadku poleceń przelewu SEPA bank beneficjenta musi mieć siedzibę w jednym z 28 państw będących członkiem Unii Europejskiej lub w jednym z czterech państw Europejskiego Stowarzyszenia Wolnego Handlu (Islandia, Liechtenstein, Norwegia, Szwajcaria), w Monako lub w San Marino.

B. Polecenie zapłaty (Klient jako wierzyciel)

Bank – jako bank Klienta – obsługuje dyspozycje polecenia zapłaty otrzymywane od Klienta w celu pobrania środków pieniężnych z rachunku bankowego płatnika.

Na wniosek Banku Klient składa zgodę otrzymaną od płatnika. Jest to zgoda płatnika na obciążanie jego rachunku kwotami poleceń zapłaty opartymi na jego zobowiązaniach wobec Klienta. Zgoda jest przekazywana Klientowi lub bankowi płatnika w formie pisemnej lub w innej formie uzgodnionej z bankiem płatnika lub z Klientem. Zgody muszą obejmować co najmniej trzy elementy: niepowtarzalny identyfikator płatnika, niepowtarzalny identyfikator Klienta i niepowtarzalny identyfikator płatności.

Realizacja polecenia zapłaty

1. Przed zainicjowaniem polecenia zapłaty w Banku Klient upewnia się, że płatnicy udzielili zgody na polecenie zapłaty.
2. Bank wykonuje dyspozycję polecenia zapłaty w dniu wskazanym przez Klienta w dyspozycji jako data płatności:
 - a. dyspozycja musi być złożona przed godz. 14:30 co najmniej jeden dzień roboczy przed wskazaną datą.
 - b. w przypadku złożenia dyspozycji po godz. 14:30 dnia roboczego poprzedzającego wskazaną datę, dyspozycja jest wykonywana w dniu roboczym następującym po wskazanej dacie płatności.
 - c. gdy wskazana data płatności przypada w tym samym dniu, w którym została złożona dyspozycja, lub w dniu, który minął, a dyspozycja została złożona przed godz. 14:30, dyspozycja jest wykonywana przez Bank następnego dnia roboczego. W przypadku złożenia dyspozycji po godz. 14:30 dyspozycja jest wykonywana drugiego dnia roboczego po jej złożeniu.

- d. gdy data płatności nie jest dniem roboczym, dyspozycja jest wykonywana przez Bank następnego dnia roboczego.
3. Klient może anulować dyspozycję polecenia zapłaty złożoną w Banku najpóźniej dwa dni robocze przed datą płatności wskazaną w dyspozycji polecenia zapłaty, do godz. 10:00.
4. Kwota płatności z tytułu polecenia zapłaty jest udostępniana Klientowi na Rachunku następnego dnia roboczego po otrzymaniu środków pieniężnych z banku płatnika.
5. Klientowi przesyłane są raporty ze zrealizowanych z powodzeniem poleceń zapłaty. Specyfikacje w zakresie formatu i dostarczania tych raportów określa Wniosek o uruchomienie produktu.
6. Klient zawiadamia Bank o wszelkich rozbieżnościach pomiędzy raportem a wyciągiem z rachunku w terminie 14 dni od otrzymania raportu.
7. Bank płatnika może odmówić wykonania otrzymanej dyspozycji polecenia zapłaty z któregośkolwiek z następujących powodów:
 - a. Płatnik nie złożył w swoim banku zgody lub zablokował korzystanie z poleceń zapłaty;
 - b. Płatnik skutecznie odwołał wcześniej złożoną w banku zgodę;
 - c. Środki pieniężne dostępne na rachunku bankowym płatnika są niewystarczające do tego, żeby pokryć polecenie zapłaty, lub zostały zajęte przez uprawnione do tego organy;
 - d. Rachunek bankowy płatnika został zamknięty;
 - e. Płatnik złożył w banku dyspozycję odwołania niezrealizowanego polecenia zapłaty;
 - f. Bank płatnika nie oferuje swoim klientom rozliczeń w formie polecenia zapłaty.

Jeżeli płatnik złożył dyspozycję zwrotu wykonanego polecenia zapłaty (w terminach przewidzianych w przepisach prawa lub warunkach stosowania polecenia zapłaty wynikających z porozumienia międzybankowego w sprawie stosowania polecenia zapłaty) lub jeżeli płatnik nie udzielił zgody na polecenie zapłaty, Bank obciąża rachunek Klienta kwotą wykonanego polecenia zapłaty wraz z odsetkami wynikającymi z umowy rachunku bankowego płatnika (w tym również w ciężar udzielonego przez Bank limitu kredytu w rachunku). Bank może wymagać złożenia przez Klienta oświadczenia o poddaniu się egzekucji zgodnie z art. 777 kodeksu postępowania cywilnego. W przypadku krajowych poleceń zapłaty bank dłużnika musi mieć siedzibę w Polsce.

C. Wpłaty w Banku

Klient może fizycznie zdeponować czeki i wpłacić gotówkę w dowolnym oddziale Banku. Przyjmowane mogą być banknoty walut obcych. Lista walut obcych przyjmowanych przez Bank – patrz strony internetowe Banku.

D. Wpłaty gotówkowe

Bank oferuje wpłaty gotówkowe za pośrednictwem wyspecjalizowanych dostawców usług w formie otwartej (gotówka liczona w obecności Klienta) lub w formie zamkniętej (środki pieniężne w bezpiecznych kopertach; gotówka liczona pod nieobecność Klienta).

Wpłaty gotówki w formie otwartej mogą być dokonywane:

- w placówce Banku, w walucie krajowej (w bilonie i banknotach) lub obcej (w banknotach). Lista walut obcych akceptowanych przez Bank jest dostępna na stronie internetowej Banku. Rachunek klienta jest uznawany bezzwłocznie.
- w placówkach Poczty Polskiej wymienionych na stronie internetowej (www.poczta-polska.pl), z wyjątkiem placówek oznaczonych jako agencje pocztowe, wyłącznie w PLN, uruchomienie po upływie 15 dni od daty złożenia odpowiedniego Wniosku o uruchomienie produktu. W przypadku wpłaty dokonanej do godz. 14:00 w dniu roboczym, księgowanie na rachunku nastąpi w tym samym dniu. W przypadku otrzymania wpłaty po godz. 14:00 w dniu roboczym lub w dniu innym niż dzień roboczy będzie ona zaksięgowana na rachunku następnego dnia roboczego.

Wpłaty gotówki w formie zamkniętej mogą być dokonywane:

- w Automatycznych Maszynach Depozytowych (ADM), w PLN (banknoty/bilon) lub walutach obcych (tylko banknoty) akceptowanych przez Bank. Bank dostarcza kurierem numery PIN, karty dostępu i klucze umożliwiające korzystanie z wpłatomatu.
- w Jednostkach Liczących (Sortownie), dedykowane lokalizacje dostawców usług, aktualna lista jednostek liczących udostępniana na żądanie, w PLN (bilon/banknoty) lub walutach obcych (tylko banknoty) akceptowanych przez Bank, przy czym bilon nie może przekraczać 5% wartości wpłaty, uruchomienie po upływie 7 dni od daty złożenia odpowiedniego Wniosku o uruchomienie produktu.
- w wybranych Urzędach Poczтовых (Wpłaty Plus), wybrane lokalizacje Poczty Polskiej, tylko w PLN, przy czym bilon nie może przekraczać 5% wartości wpłaty, uruchomienie po upływie 10 dni od daty złożenia odpowiedniego Wniosku o uruchomienie produktu.

Proces wpłaty gotówki w formie zamkniętej

1. Transport wpłat gotówkowych może być zapewniany na podstawie odrębnej umowy pomiędzy Klientem a dostawcą usług transportu środków pieniężnych. Transakcję wpłaty gotówkowej uznaje się za autoryzowaną od momentu dostarczenia do Jednostki Liczącej, pracownika Poczty Polskiej lub ADM.
2. Klient wypełnia Bankowy Dowód wpłaty (eBDW) dla poszczególnych wpłat gotówkowych, wskazując deklarowaną wartość danej wpłaty gotówkowej i rachunek do uznania. Oprogramowanie do tworzenia eBDW jest dostępne bezpłatnie na stronach internetowych Banku (<http://www.citibank.pl/poland/corporate/polish/wplaty-gotowkowe.htm>). Przed zainstalowaniem oprogramowania Klient sporządzi kopie bezpieczeństwa wszystkich programów i baz danych na sprzęcie komputerowym, na którym ma być zainstalowane oprogramowanie.

Wymagania w zakresie opakowań dla wpłat gotówkowych w formie zamkniętej

- a. Pojedyncza bezpieczna koperta zawiera banknoty o wartości nie niższej niż 5000 PLN. Banknoty o tym samym nominale są ujęte w opaski po 100 sztuk lub opaską jest ujęta cała wpłata w taki sposób, aby banknoty nie mogły się względem siebie przemieszczać. Na opasce podana jest data wpłaty, liczba banknotów, wartość nominału i kwotę przeliczeniową. Bank nie przyjmuje banknotów, które są nadmiernie zużyte, zniszczone, lub noszą nieczytelne numery lub kody seryjne.
 - b. Bilon jest pakowany w woreczki lub rulony. Na przywieszce woreczka lub rulonu podana jest data wpłaty, liczba monet, nominał i wartość przeliczeniową. Nie są przyjmowane monety nadmiernie zużyte, zniszczone, skorodowane lub wytarte.
 - c. Waluty są pakowane oddzielnie.
 - d. Poszczególne pakiety wpłat muszą być zabezpieczone w sposób zapobiegający ich otwarciu bez widocznego naruszenia opakowania.
 - e. Poszczególne pakiety są oznaczone nazwą Klienta, nazwą jednostki Banku przyjmującej wpłatę oraz numerem identyfikacyjnym pakietu.
 - f. Do każdego pakietu musi być przymocowany jeden egzemplarz eBDW, który musi być widoczny bez otwierania pakietu. Drugi egzemplarz eBDW powinien być umieszczony wewnątrz pakietu. Zawartość pakietu powinna odpowiadać wartości i specyfikacji na eBDW.
3. Jeśli kwota wyrażona cyframi na eBDW jest inna niż kwota podana słownie, Bank za wiążącą uznaje kwotę wyrażoną słownie. W przypadku jakichkolwiek rozbieżności między treścią oryginału i kopii eBDW, Bank uznaje za sformułowanie wiążące treść oryginału.
 4. Zużyte lub zniszczone monety i banknoty PLN są zwracane klientowi oraz wystawiany jest Protokół Stwierdzenia Różnicy w zakresie rozbieżności. Bank przekazuje zużyte i zniszczone banknoty i monety do Narodowego Banku Polski. Zużyte i zniszczone banknoty i monety, których nie wymieni Narodowy Bank Polski, muszą zostać odebrane przez Klienta z miejsca wskazanych przez Bank.
 5. Zużyte i zniszczone banknoty i monety walut obcych będą odrzucane i powinny zostać niezwłocznie odebrane przez Klienta (najpóźniej w ciągu dwóch tygodni od zawiadomienia).
 6. Bilon w walutach obcych może nie zostać przyjęty. W przypadku przyjęcia Bank może zmienić wysokość opłaty manipulacyjnej określonej w tabeli prowizji i opłat bankowych.
 7. Rachunek klienta jest uznawany zgodnie z formą księgowania wpłaty (kwotą po przeliczeniu lub deklarowaną):

Terminy uznawania rachunku			
ADM	Jednostka Licząca (otwarta w dni robocze)	Jednostka Licząca (otwarta przez całą dobę)	Poczta Polska (Wpłaty Plus)
Kwotą przeliczoną			
Dostarczone do godz. 8:00 dnia roboczego: księgowane tego samego dnia Dostarczone po godz. 8:00: księgowane następnego dnia roboczego Wyjątek: Wpłaty zdeponowane w ADM w Słupsku są uznawane na rachunku drugiego dnia roboczego	Dostarczone do godz. 13:00 dnia roboczego: księgowane tego samego dnia Dostarczone po godz. 13:00: księgowane następnego dnia roboczego	Dostarczone do godz. 13:00 dnia roboczego: księgowane tego samego dnia Dostarczone po godz. 13:00: księgowane następnego dnia roboczego	Dostarczone do godz. 7:00 dnia roboczego: środki pieniężne są przelewane na rachunek tego samego dnia Dostarczone po godz. 7:00: środki pieniężne są przelewane na rachunek następnego dnia roboczego
Kwotą deklarowaną			
Dostarczone przed godz. 8:00 dnia roboczego: księgowane tego samego dnia Dostarczone po godz. 8:00 : księgowane następnego dnia roboczego	Dostarczone przed godz. 14:00 dnia roboczego: księgowane tego samego dnia Dostarczone po godz. 14:00 dnia roboczego: księgowane do godz. 12:00 następnego dnia roboczego po dniu wpłaty	Dostarczone do godz. 7:00 dnia roboczego: księgowane do godz. 12:00 w dniu wpłaty Dostarczone po godz. 7:00, ale przed godz. 14:00 w dniu roboczym: księgowane w dniu wpłaty Dostarczone po godz. 14:00: księgowane do godz. 12:00 następnego dnia roboczego po wpłacie	

Jeżeli Bank zmieni lokalizację Jednostki Liczącej lub ADM, Klient zostanie poinformowany o tym fakcie z wyprzedzeniem listownie lub emailiem.

Protokoły Stwierdzenia Różnicy są sporządzane dla wszystkich rozbieżności gotówkowych większych lub równych 50 PLN dla wpłat gotówkowych w PLN i dla rozbieżności o każdej wartości dla wpłat gotówkowych w walutach obcych. Protokoły Stwierdzenia Różnicy są przekazywane przez CitiDirect BE[®] lub emailiem na adres określony we Wniosku o uruchomienie produktu.

Wyciągi bankowe i kopie Protokołów Stwierdzenia Różnicy (w przypadku stwierdzenia fałszywych monet lub banknotów lub rozbieżności między wartością zadeklarowaną na

dowodzie wpłaty a faktyczną wartością w pakiecie) stanowią wyłączny dowód wpłaty gotówkowej i potwierdzenie uznania rachunku Klienta.

Jeśli na bankowym dowodzie wpłaty (eBDW/BDW) wskazany jest inny rachunek niż w odpowiednim Wniosku o uruchomienie produktu lub jeśli rachunek wskazany na Bankowym Dowodzie Wpłaty jest nieprawidłowy, odpowiedni rachunek prowadzony w danej walucie zostaje uznany zgodnie z Wnioskiem o uruchomienie produktu.

Bezpieczne koperty do wpłat zamkniętych

Bank oferuje bezpieczne jednorazowe koperty zaopatrzone w wysokiej jakości taśmę samoklejącą z tworzywa sztucznego, uniemożliwiającą otwarcie opakowania bez jego widocznego naruszenia. Pakiety bezpiecznych kopert są wysyłane kurierem na zamówienie Klienta na adres w Polsce.

Zamówienia do 3000 kopert złożone do godz. 15:30 dnia roboczego są wysyłane kurierem następnego dnia roboczego. Zamówienia poniżej 3000 kopert złożone po godz. 15:30 są wysyłane kurierem dwa dni robocze później.

Zamówienia powyżej 3000 kopert wymagają dłuższego czasu realizacji (do pięciu dni roboczych). Klient otrzymuje email z potwierdzeniem spodziewanej daty dostawy.

E. SpeedCollect

SpeedCollect umożliwia Klientom identyfikację i uzgodnienie dużej liczby płatników w różnych kanałach płatniczych i sieciach bankowych.

SpeedCollect opiera się na rachunkach wirtualnych, które są 26-cyfrowymi numerami rachunków zgodnymi z normami NRB i IBAN, znanych płatnikom Klienta, na które dokonywane są wpłaty. Numer rachunku wirtualnego składa się z trzech kolejnych elementów: XX CCCC CCCC CCCC IIII IIII IIII.

- Cyfry X to 2-cyfrowa suma kontrolna, obliczana za każdym razem przez Klienta poprzez użycie algorytmu NRB/IBAN na podstawie pozostałych cyfr.
- Cyfry C są przypisywane Klientowi przez Bank podczas wdrożenia. Jest to stała część, zwykle złożona z 12 cyfr.
- Cyfry I są określane jako Infokod. Są one każdorazowo przypisywane przez Klienta w celu identyfikacji poszczególnych płatników (lub innych jednostek, np. zamówień, faktur, placówek itd.). Infokod prezentowany jest w raportach i zazwyczaj składa się z 12 cyfr.

Za pośrednictwem rachunków wirtualnych SpeedCollect mogą być dokonywane wpłaty w postaci przelewów lokalnych, przelewów wysokokwotowych, przelewy zagraniczne, w tym SEPA, jak również wpłaty gotówkowe.

Uzgodnienia przed uruchomieniem usługi

Klient kontaktuje się z Bankiem w celu uruchomienia usługi SpeedCollect. Klient wraz z Bankiem uzgadniają:

1. stałą część numeracji rachunków wirtualnych, tzn. cyfry części C;
2. numer rachunku rzeczywistego, na którym będą księgowane wpłaty SpeedCollect;

3. metodę księgowania wpłat (z konsolidacją lub bez);
4. raportowanie: Bank przedstawia Klientowi przykładowe raporty SpeedCollect, z których Klient wybiera preferowany format lub uzgadnia z Bankiem niestandardowy format raportu i terminy jego dostarczania.

Korzystanie z usługi

1. Klient generuje wirtualny numer rachunku SpeedCollect i przekazuje go płatnikowi (np. drukuje numer na fakturze doręczanej płatnikowi).
2. Płatnik dokonuje wpłat na wirtualny numer rachunku SpeedCollect.
3. Bank otrzymuje wpłatę i sprawdza odpowiedni numer rachunku rzeczywistego, a następnie:
 - a. W przypadku wpłat nieobjętych konsolidacją, Bank księguje każdą wpłatę osobno. Infokod widoczny jest na wyciągu bankowym oraz w raporcie SpeedCollect.
 - b. W przypadku wpłat objętych konsolidacją, Bank księguje wpłaty jako kwotę zbiorczą. Takie płatności są wykazywane na wyciągu bankowym zbiorczo (jedno zbiorcze księgowanie po każdej sesji rozliczeniowej Elixir). Szczegóły poszczególnych wpłat nie są widoczne na wyciągu ani w raporcie SpeedCollect, dlatego Bank dostarcza dodatkowe raporty (tzn. pliki DCH) zawierające szczegóły. Jednakże księgowanie zbiorcze jest możliwe tylko w przypadku przelewów lokalnych. Niektóre transakcje (np. transakcje w walutach obcych, wpłaty gotówkowe lub Express Elixir realizowany w mechanizmie podzielonej płatności) są wyłączone z konsolidacji i księgowane osobno.
4. Bank dostarcza raporty SpeedCollect, których treść może się różnić od wyciągów bankowych.
5. Bank może też wysyłać SMS-y na numery telefonów polskich operatorów sieci komórkowych. SMS-y takie stanowią niestandardową formę raportu SpeedCollect.
6. W przypadku zamknięcia rachunku rzeczywistego wskazanego dla wpłat SpeedCollect i złożenia przez Klienta w Banku dyspozycji dotyczącej rachunku rzeczywistego (np. przekierowania wpływów), dyspozycja ta dotyczy tylko rachunku rzeczywistego, a nie rachunków wirtualnych SpeedCollect.

F. ARMS (*Account Receivables Matching Service*)

Usługa ARMS to rozwiązanie zapewniające Klientowi raportowanie transakcji dostosowane do indywidualnych potrzeb.

W szczególności usługę ARMS można wykorzystywać do uzgadniania transakcji przychodzących ze spodziewanymi. Połączenie szerokiego zakresu dostępnych kanałów i metod płatności ze wzbogaconymi danymi transakcyjnymi umożliwia wystandaryzowaną sprawozdawczość, a tym samym znacznie upraszcza procesy uzgadniania należności.

Uzgodnienia przed uruchomieniem usługi

1. Klient kontaktuje się z Bankiem w celu uruchomienia usługi ARMS. Klient wraz z Bankiem uzgadniają:
 - a. dane wejściowe: informacje, które będą stosowane do uzgodnień. Dla uzgodnień statycznych, dane wejściowe opierają się na informacjach dostępnych w Banku (np. raport MT940). Dla uzgodnień dynamicznych, dane wejściowe opierają się na informacjach dostarczanych przez Klienta (np. codzienna baza danych o płatnościach oczekiwanych), które mogą być zestawiane np. z raportem MT940;
 - b. logikę przetwarzania: w jaki sposób dane wejściowe powinny być przetwarzane na dane wyjściowe, w tym: logika biznesowa, wartości progowe, warunki i częstotliwość;
 - c. dane wyjściowe: Klient otrzymuje ostateczny raport, przedstawiający dane wejściowe przetworzone zgodnie z logiką przetwarzania;
 - d. kanały dostępu: kanały, które będą wykorzystywane do transmisji danych wejściowych i wyjściowych;
 - e. proces wdrożenia, łącznie z testowaniem rozwiązania.
2. Warunkiem rozpoczęcia wdrożenia usługi może być podpisanie przez Klienta umowy o zachowaniu poufności.

Korzystanie z usługi

1. W przypadku uzgodnień dynamicznych, Klient przygotowuje swoje dane wejściowe i przesyła je uzgodnionym kanałem dostępu do Banku.
2. Bank przetwarza dane wejściowe na dane wyjściowe zgodnie z uzgodnioną logiką przetwarzania.
3. Bank przygotowuje dane wyjściowe i przesyła je uzgodnionym kanałem dostępu do Klienta.

IV. Pozostałe kwestie

1. Klient dokonuje własnej oceny prawnych, regulacyjnych, podatkowych i księgowych efektów usług.
2. Taryfy opłat, procedury, wymagania, przewodniki, podręczniki i inne materiały opisujące procedury, wymagania i ograniczenia dotyczące korzystania z usług mogą być zmieniane o czym Bank poinformuje Klienta.
3. Rozliczenie płatności i wierzytelności podlega zasadom ustalonym przez odpowiedni system rozliczeniowy. Zarówno Bank, jak i jego klienci muszą stosować się do tych zasad rozliczeniowych.
4. Dni robocze oznaczają dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
5. Dzień operacyjny oznacza czas, podczas którego Bank przyjmuje i przetwarza polecenia i dyspozycje. Polecenia i dyspozycje nie są przyjmowane poza dniami operacyjnymi. Godziny operacyjne są zdefiniowane jako okres czasu (stosownie do godzin granicznych podanych na stronie www.citihandlowy.pl/strefaklienta) w dniu operacyjnym i mogą być różne dla różnych rodzajów dyspozycji i usług.
6. Bank podejmuje starania, aby wszelkie kompletne dyspozycje i zlecenia płatnicze otrzymane przez Bank w godzinach operacyjnych przetwarzane były tego samego dnia. Na żądanie dyspozycje płatnicze będą inicjowane określonego dnia lub z końcem określonego okresu.
7. W przypadku, gdy środki zgromadzone na Rachunku nie są wystarczające do zrealizowania dyspozycji Klienta, wykonanie dyspozycji płatniczej rozpocznie się, a tym samym dyspozycję uznaje się za otrzymaną, w dniu, w którym środki na Rachunku będą wystarczające do jej zrealizowania, z zastrzeżeniem, że środki powinny być dostępne na Rachunku w terminie 3 dni roboczych od dostarczenia przez Klienta dyspozycji płatniczej do Banku.
8. Kompletne dyspozycje i zlecenia (w tym dotyczące płatności podatków i innych zobowiązań publicznoprawnych) otrzymane po godzinach operacyjnych są traktowane jako przyjęte i przetwarzane następnego dnia operacyjnego. Niekompletne dyspozycje i zlecenia otrzymane przez Bank w dniu operacyjnym są odrzucane.
9. Klienci mają obowiązek podawać cel płatności i przelewów. Cel przelewu lub płatności muszą potwierdzać odpowiednie dokumenty. Godziny przyjmowania dyspozycji określają godziny operacyjne.
10. Bardziej szczegółowe informacje na temat godzin granicznych, kwot maksymalnych, kursów, opłat i danych kontaktowych znajdują się na stronach internetowych Banku pod adresem: www.citihandlowy.pl/strefaklienta. Podręczniki użytkownika dotyczące CitiDirect BE[®] są dostępne na stronach www.citidirect.pl.
11. Przed upływem okresu wypowiedzenia Klient jest zobowiązany przekazać Bankowi dyspozycję zadysponowania środkami zgromadzonymi na rachunku. Jeżeli saldo rachunku VAT Klienta jest w dacie wygaśnięcia dodatnie, Bank czeka na potwierdzenie

decyzji Naczelnika Urzędu Skarbowego co do zadysponowania środkami. W przypadku braku takiej informacji Bank utrzymuje nieoprocentowany rachunek VAT do czasu otrzymania przez Bank informacji o decyzji Naczelnika Urzędu Skarbowego i jej wykonaniu. Bank nie pobiera od tych rachunków żadnych opłat ani prowizji, ani nie wykonuje w odniesieniu do nich żadnych dyspozycji płatniczych. Po otrzymaniu przez Bank zgody Naczelnika Urzędu Skarbowego na przelew środków zgromadzonych na rachunku VAT Klienta na jego rachunek rozliczeniowy Bank niezwłocznie wykonuje taką dyspozycję i przelewa środki z rachunku rozliczeniowego Klienta na wskazany przez niego inny rachunek. Po wykonaniu tych dyspozycji rachunek rozliczeniowy i związany z nim rachunek VAT zostaje natychmiast zamknięty.

V. Formularze elektroniczne

Bank oferuje użytkownikom CitiDirect BE[®] dostęp do platformy wymiany formularzy elektronicznych.

Formularze elektroniczne pozwalają użytkownikom znacznie ograniczyć ilość wymienianej z Bankiem dokumentacji papierowej.

Bank zapewnia usługi formularzy elektronicznych po wypełnieniu przez Klienta odpowiedniego Wniosku o uruchomienie produktu. Klient upoważnia konkretnych użytkowników do autoryzacji formularzy elektronicznych.

VI. Skonsolidowane procedury bezpieczeństwa Bankowości Transakcyjnej

Zgodnie z informacjami w punkcie „Komunikacja” Ogólnych Warunków Prowadzenia Rachunków i Świadczenia Usług (lub innymi mającymi zastosowanie warunkami prowadzenia rachunków) („Ogólne Warunki”) przyjętych przez Bank i przez Klienta – to, co jest zawarte poniżej, to opis procedur bezpieczeństwa („Procedury”) stosowanych w rozwiązaniach Bankowości Transakcyjnej (*Treasury and Trade Solutions*, TTS) Banku w związku z następującymi Usługami lub kanałami dostępu:

- CitiDirect BE[®] (w tym Elektroniczne Zarządzanie Rachunkami Bankowymi (*Electronic Bank Account Management*, eBAM), TreasuryVision[®] oraz WorldLink[®]) Interaktywny system odpowiedzi głosowej (*Interactive Voice Response*, „IVR”)
- Email/faks z Banku z wyjątkiem ręcznie inicjowanego przelewu (*Manually Initiated Funds Transfer*, „MIFT”)
- CitiConnect[®]
- Inne lokalne elektroniczne kanały dostępu

Dostępność poszczególnych usług i kanałów dostępu może być różna na lokalnych rynkach. Niniejsze Procedury mogą być aktualizowane za powiadomieniem Klienta drogą elektroniczną lub inną. Dalsze korzystanie przez Klienta z którychkolwiek usług lub kanałów dostępu, o których mowa wyżej, po otrzymaniu informacji o aktualizacji Procedur (co może obejmować, między innymi, zamieszczenie zaktualizowanych Procedur w systemie CitiDirect BE[®] w związku z daną usługą lub danym kanałem dostępu) oznacza przyjęcie przez Klienta takich zaktualizowanych Procedur. Z niniejszymi Procedurami należy się zapoznawać łącznie z Ogólnymi Warunkami, które mogą być aktualizowane. Terminy pisane wielką literą i inaczej nie zdefiniowane w niniejszym dokumencie mają znaczenie przypisane im w Ogólnych Warunkach Prowadzenia Rachunków i Świadczenia Usług.

A. Role i obowiązki Administratora Systemu*

W przypadku CitiDirect BE[®] Bank wymaga wskazania co najmniej dwóch różnych osób, które będą wprowadzać i autoryzować dyspozycje w systemie. W związku z tym konieczne jest wyznaczenie co najmniej dwóch Administratorów Systemu, którzy działając razem, będą w stanie wydawać przez kanały dostępu dyspozycje związane z każdą realizowaną funkcją administracyjną lub w związku z komunikacją z Bankiem przez Internet. Wszelka taka Komunikacja, autoryzowana przez dwóch Administratorów Systemu, zostanie zaakceptowana przez Bank i Bank podejmie w związku z tym dalsze działania. Bank zaleca wyznaczenie co najmniej trzech Administratorów Systemu w celu zapewnienia odpowiedniego wsparcia w wyjątkowych sytuacjach. Klient wskazuje swoich Administratorów Systemu na właściwym wniosku Bankowość Transakcyjna – Formularz Aktywacji. Administrator Systemu może również działać jako administrator podmiotu trzeciego (np. jednostki powiązanej z Klientem) i egzekwować wszelkie związane z tym prawa (łącznie z ustalaniem uprawnień użytkowników danego podmiotu do Rachunków),

bez jakiegokolwiek dalszego upoważnienia, jeżeli dany podmiot trzeci wystawia formularz Upoważnienie do dostępu (UAA) (lub inny sposób akceptowany przez Bank) dający Klientowi dostęp do jego Rachunków. Ma to zastosowanie wyłącznie do Rachunków, których dotyczy dane upoważnienie.

**Na niektórych lokalnych rynkach role i obowiązki Administratorów Systemu mogą być zakazane. W sprawie dalszych informacji prosimy o kontakt z przedstawicielem Obsługi Klienta.*

Funkcja Administratora Systemu obejmuje m.in.:

1. Ustalanie i utrzymywanie dostępu i uprawnień użytkowników (w tym samych Administratorów Systemu), łącznie z działaniami takimi jak:
 - (a) tworzenie, usuwanie i modyfikowanie profili użytkowników (w tym profili administracyjnych) oraz ich uprawnień (należy pamiętać, że imię/nazwisko użytkownika musi być zgodne z odpowiednimi dokumentami tożsamości)
 - (b) budowanie profili dostępu definiujących funkcje i dane dostępne dla różnych użytkowników, oraz
 - (c) włączanie i wyłączanie narzędzi uwierzytelniających użytkowników podczas logowania
2. Tworzenie i modyfikowanie wpisów w bibliotekach utrzymywanych przez Klienta (np. bibliotekach beneficjentów lub szablonów płatności) i upoważnianie do tego innych użytkowników
3. Modyfikowanie schematów autoryzacji płatności
4. Przypisywanie narzędzi uwierzytelniających generujących hasła w sposób dynamiczny lub innych narzędzi umożliwiających dostęp do systemu użytkownikom Klienta
5. Zawiadamianie Banku w przypadku jakiegokolwiek podejrzenia, że zostało naruszone bezpieczeństwo

Administratorzy Systemu mogą również ustalać limity transakcyjne dla użytkowników, dla tych produktów Banku, do których ma dostęp Klient. Limity te nie są monitorowane ani weryfikowane przez Bank; Klient powinien je monitorować w celu zapewnienia zgodności z wewnętrznymi zasadami i wymogami Klienta, w tym między innymi ustalonymi przez Zarząd lub Radę Nadzorczą Klienta lub równoważnymi.

W odniesieniu do Usługi eBAM wymagane są następujące role:

1. Specjalista ds. Bezpieczeństwa: pełni funkcje opisane powyżej w punktach (1) A–C w opisie ról Administratorów Systemu
2. Sekretarz: zapewnia zgodność Procesów, Użytkowników wyznaczonych jako Osoby Autoryzujące oraz ich przypisania do Procesów z wewnętrznymi zasadami polityki i wymogami oraz poziomami uprawnień i zatwierdzeń ustalonymi przez Zarząd lub Radę Nadzorczą Klienta (i Właścicieli Rachunku) lub równoważny organ.
3. Wyznaczona Osoba Autoryzująca: ma szerokie, nadrzędne uprawnienia do inicjacji i autoryzacji działań w ramach Procesów

4. Inicjatorzy Dyspozycji: osoby upoważnione do wykonywania działań administracyjnych, takich jak wprowadzanie dyspozycji zarządzania podpisującymi i rachunkami do systemu eBAM

Zadania Specjalistów ds. Bezpieczeństwa, Sekretarza i Wyznaczonych Osób Autoryzujących:

- a) Definiowanie konfiguracji hierarchii i nadzoru nad lokalizacjami/procesami oraz administrowanie nimi; w szczególności ustalanie Procesów oraz identyfikacja Użytkowników i poziomów zatwierdzeń
- b) Tworzenie dodatkowych stanowisk Starszych Administratorów i przypisywanie do nich Użytkowników (którzy mogą – ale nie muszą – być pracownikami Klienta)
- c) Zawiadamianie Banku w przypadku jakiegokolwiek powodu do podejrzeń, że zostało naruszone bezpieczeństwo lub poufność danych uwierzytelniających w przypadku któregoś z Użytkowników (w tym Starszych Administratorów)
- d) Tam, gdzie to istotne, wypełnianie, zmienianie, zatwierdzanie lub uzupełnianie formularzy wdrożeniowych Klienta, których Bank może w uzasadniony sposób od czasu do czasu wymagać w związku ze świadczeniem usług i dostarczaniem produktów dla Klienta.

B. Metody Uwierzytelniania

Procedury obejmują bezpieczne metody uwierzytelniania („Metody Uwierzytelniania”) stosowane w celu jednoznacznego ustalania tożsamości i weryfikacji uprawnień Klienta i/lub któregoś z jego użytkowników najczęściej za pomocą takich mechanizmów jak pary ID Użytkownika – hasło, certyfikaty cyfrowe oraz tokeny bezpieczeństwa (realizowane sprzętowo lub programowo) generujące dynamiczne hasła stosowane do dostępu do usług lub kanałów dostępu za każdym razem, gdy Klient lub użytkownik loguje się lub uwierzytelnia. Proszę zwrócić uwagę, że dostępność opisanych niżej Metod Uwierzytelniania różni się w zależności od lokalnego rynku.

Administratorzy Systemu i inni użytkownicy, którzy chcą (a) zainicjować lub zautoryzować transakcję (i których Profil Użytkownika to umożliwia) lub (b) uzyskać dostęp do systemu zgodnie z uprawnieniami, muszą posłużyć się Metodami Uwierzytelniania (które mogą być aktualizowane, jak opisano wyżej).

Następujące Metody Uwierzytelniania, łącznie z identyfikatorem użytkownika, są dostępne w celu zalogowania do wymienionych wyżej usług lub kanałów dostępu:

Metoda Uwierzytelniania	Opis
Token: zapytanie– odpowiedź	Zabezpieczony 4 – cyfrowym numerem PIN: (i) token mobilny (np.aplikacja MobilePASS), albo (ii) token fizyczny (np. SafeWord Card, Vasco), każdorazowo stosowany w celu wygenerowania dynamicznego hasła. Podczas logowania do CitiDirect BE system generuje zapytanie, a wygenerowane tokenem hasło jest wprowadzane wprowadzane do systemu.
Token: jednorazowe hasło	Zabezpieczony 4 – cyfrowym numerem PIN: (i) token mobilny (np.aplikacja MobilePASS), albo (ii) token fizyczny (np. SafeWord Card, Vasco), każdorazowo stosowany w celu wygenerowania dynamicznego hasła. Podczas logowania do CitiDirect BE system generuje zapytanie, a wygenerowane tokenem hasło jest wprowadzane wprowadzane do systemu.
SMS: jednorazowy kod	Dynamiczne hasło jest przesyłane użytkownikowi przez SMS, po czym użytkownik wprowadza je do systemu podczas logowania.
Jednorazowy kod otrzymany głosowo przez telefon	Hasło jest podawane użytkownikowi telefonicznie przez automat głosowy, po czym użytkownik wprowadza je do systemu podczas logowania.
Uwierzytelnianie wielostopniowe	Podczas logowania do systemu wprowadzane jest zarówno hasło generowane dynamicznie z wykorzystaniem tokena jak i hasło statyczne, w którego posiadaniu jest użytkownik.
Certyfikaty cyfrowe	Do uwierzytelnienia stosowany jest certyfikat cyfrowy wydawany przez zatwierdzone centrum certyfikacji. Certyfikaty cyfrowe wykorzystują mechanizm Magazynu Kluczy i przypisanych do niego kodów PIN. Mogą być wydawane przez IdenTrust, SWIFT (3SKey) lub innych uzgodnionych dostawców.
Statyczne hasło	Podczas logowania użytkownik wprowadza hasło statyczne. Hasło statyczne zazwyczaj ogranicza możliwości użytkownika w systemie w ten sposób, że informacje mogą być przeglądane, ale nie są uruchamiane żadne możliwości transakcyjne.
Interaktywna obsługa głosowa („IVR”) i email	Użytkownicy kontaktujący się z bankiem będą poproszeni o podanie numeru PIN lub innej informacji w celu weryfikacji ich dostępu przez telefon lub przez email.
Faks	Dla każdej korespondencji otrzymywanej przez Bank, z wyjątkiem dyspozycji MIFT, będziemy weryfikować podpisy zgodnie z reprezentacją prawną.
MTLS	Protokół <i>Mandatory Transport Layer Security</i> (MTLS) tworzy bezpieczne, prywatne połączenie emailowe pomiędzy bankiem a podmiotem zewnętrznym. Email wysyłany jest przez Internet, specjalnie stworzonym na ten cel i szyfrowanym protokołem TLS kanałem.
Bezpieczny PDF	Zaszyfrowane wiadomości email dostarczane są do skrzynki odbiorczej jako dokumenty PDF zabezpieczone przed otwarciem prywatnym hasłem. Zaszyfrowana jest zarówno treść wiadomości, jak i wszelkie dołączone pliki. Prywatne hasło musi być ustawione po odebraniu pierwszego bezpiecznego emaila.

Szczegółowe informacje na temat którejkolwiek z tych Metod Uwierzytelniania, dostępne są w sekcji Pomoc w logowaniu na stronie CitiDirect BE® (<https://portal.citidirect.com/portalservices/forms/loginHelp.pser>).

Dla CitiConnect:

- Jeżeli Klient do połączenia się z Bankiem wybierze publiczne połączenie internetowe, w tym HTTPS, bezpieczne FTP lub FTPS, Bank i Klient wymienią certyfikaty bezpieczeństwa w celu zapewnienia pełnego szyfrowania i bezpieczeństwa zarówno kanału komunikacji, jak i wymienianych wiadomości. Bank przyjmuje Komunikację wyłącznie pochodzącą z bezpiecznej bramki komunikacyjnej Klienta przy użyciu wymienionych certyfikatów bezpieczeństwa, i odwrotnie, i wysyła tylko Komunikację do bezpiecznej bramki komunikacyjnej Klienta przy użyciu wymienionych certyfikatów bezpieczeństwa.
- Jeżeli Klient wybierze korzystanie z CitiConnect przez SWIFT, wówczas dla wszelkich dyspozycji i poleceń płatniczych obejmujących SWIFT, w tym zmieniających lub anulujących takie polecenia, Procedury stosowane do weryfikacji, że polecenie płatnicze lub dyspozycja pochodzi od Klienta i została autoryzowana przez Klienta, są takie, jak przewidziano w Dokumentacji SWIFT (zgodnie z definicją tego terminu przyjętą przez SWIFT, z późniejszymi zmianami i uzupełnieniami), obejmującej bez ograniczeń jej Ogólne Warunki oraz Opis Usługi FIN, lub zgodnie z wszelkimi innymi warunkami, jakie mogą zostać określone przez SWIFT. Bank nie odpowiada za jakiegokolwiek błędy i opóźnienia w systemie SWIFT. Komunikacja z Bankiem powinna odbywać się zgodnie z formatem i wymaganiami określonymi przez SWIFT.
- Korzystając z VPN, zarówno Klient, jak i Bank określają jeden adres IP, z którego będzie wysyłana i odbierana Komunikacja między Klientem a Bankiem. Bank przyjmuje Komunikację wyłącznie pochodzącą ze wskazanego adresu IP Klienta, i odwrotnie, i wysyła tylko Komunikację na wskazany adres IP Klienta, i odwrotnie.
- Klient i Bank mogą również stosować sprzętowe uwierzytelnianie (*Hardware Security Module Authentication*) jako dodatek do uwierzytelniania VPN. Wymaga to, aby zarówno Bank, jak i Klient mieli zainstalowane to urządzenie na serwerach przeznaczonych do wymiany Komunikacji między Bankiem a Klientem.

Bank wymaga, aby:

- Klient chronił Metody Uwierzytelniania, łącznie z wszelkimi danymi uwierzytelniającymi do logowania lub certyfikatami bezpieczeństwa związanymi z Metodami Uwierzytelniania (łącznie – „Dane Uwierzytelniające”), i zapewnił, że dostęp do Danych Uwierzytelniających i ich rozpowszechnianie jest ograniczone wyłącznie do uprawnionych osób po stronie Klienta. Metody Uwierzytelniania i związane z nimi Dane Uwierzytelniające stanowią metody, przy pomocy których Bank weryfikuje pochodzenie Komunikacji wychodzącej od Klienta do Banku.
- Klient powinien podejmować wszelkie uzasadnione działania w celu ochrony Danych Uwierzytelniających. W związku z tym nie jest dopuszczalne, aby Klient dzielił się informacją o Danych Uwierzytelniających z inną osobą.

W pewnych jurysdykcjach (krajach) może istnieć wymóg, aby przed udzieleniem danym osobom dostępu do ustalonych funkcji, zostało potwierzone, czy osoby te spełniają wymagania przepisów prawnych dotyczących przeciwdziałania praniu pieniędzy.

Bank rozumie, że w pewnych przypadkach Klient może chcieć udostępnić Dane Uwierzytelniające Klienta podmiotowi będącemu podmiotem trzecim lub usługodawcą (w tym na przykład zewnętrznym dostawcą świadczącym obsługę płac) wskazanym przez Klienta jako podmiot upoważniony do Danych Uwierzytelniających (który to podmiot trzeci lub zewnętrzny usługodawca występuje dalej jako „Upoważniona Osoba Trzecia”) w celu uzyskania dostępu do wszelkich kanałów elektronicznych Banku i korzystania z nich w imieniu Klienta. W przypadku dokonania przez Klienta wyboru, że Dane Uwierzytelniające będą dzielone z Upoważnioną Osobą Trzecią, Bank zaleca, aby Klient podjął – i zapewnił, że każda Upoważniona Osoba Trzecia podejmie – wszelkie uzasadnione działania w celu ochrony Danych Uwierzytelniających przed ujawnieniem personelowi osoby trzeciej nie będącej Upoważnioną Osobą Trzecią. Bank jest upoważniony do działania na podstawie wszelkiej Komunikacji otrzymanej od Upoważnionej Osoby Trzeciej w imieniu Klienta zgodnie z niniejszymi Procedurami.

C. Integralność Danych i Bezpieczna Komunikacja

- Klient będzie przysyłał dane lub w inny sposób Komunikował się z Bankiem, wykorzystując Internet, email lub faks, co niekoniecznie stanowi bezpieczne systemy komunikacji i transmisji. Bank wykorzystuje wiodące metody szyfrowania (określone przez Bank), co pomaga zapewnić zachowanie poufności informacji i jej niezmiennosc podczas transmisji.
- Jeżeli Klient podejrzewa lub będzie świadomy, że istnieje wada techniczna lub niewłaściwy dostęp do kanałów dostępu, Metod Uwierzytelniania lub usług Banku lub są one niewłaściwie stosowane przez jakąkolwiek osobę (niezależnie czy jest ona upoważniona lub nie), Klient niezwłocznie powiadomi o tym Bank. W przypadku nieprawidłowości dostępu lub niewłaściwego korzystania przez jakąkolwiek osobę, Klient powinien niezwłocznie podjąć działania mające na celu zablokowanie dostępu takiej osoby.
- Jeżeli Klient podczas komunikacji z Bankiem wykorzystuje dodatkowe oprogramowanie (dostarczone przez Bank lub podmiot trzeci) do szyfrowania, formatowania plików, rozpoznawania danych oraz dyspozycji Klienta, wówczas Klient wykorzystuje to oprogramowanie wyłącznie w celu, do którego zostało zainstalowane.
- Klient akceptuje, że Bank może zawiesić dostęp Użytkowników do Usług wymagających użycia Danych Uwierzytelniających (i) w przypadku podejrzenia nieuprawnionego lub oszukańczego korzystania z tych Danych Uwierzytelniających lub (ii) w celu ochrony Usług i / lub Danych Uwierzytelniających.

VII. Podsumowanie

Dziękujemy za wybór Bankowości Transakcyjnej (*Treasury and Trade Solutions*, TTS) Banku na potrzeby zarządzania środkami finansowymi w Państwa firmie. Prosimy o kontakt z Państwa Doradcą Bankowym w sprawie jakichkolwiek kwestii dotyczących usług Bankowości Transakcyjnej.

Bankowość Transakcyjna

www.citihandlowy.pl

Wersja: Polska, wrzesień 2018 r.

Informacje zawarte w dokumencie nie stanowią porady prawnej ani podatkowej. W przypadku pytań, prosimy o kontakt z Bankiem. Dostępność produktów jest zróżnicowana w zależności od obszaru geograficznego. Wszelkie nieuprawnione użycie, powielanie lub ujawnianie jest prawnie zakazane i może skutkować pociągnięciem do odpowiedzialności.

Znaki Citi oraz Citi Handlowy stanowią zarejestrowane znaki towarowe Citigroup Inc., używane na podstawie licencji. Spółce Citigroup Inc. oraz jej spółkom zależnym przysługują również prawa do niektórych innych znaków towarowych tu użytych. Bank Handlowy w Warszawie S.A. z siedzibą w Warszawie, ul. Senatorska 16, 00-923

Warszawa, zarejestrowany w rejestrze przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr. KRS 000 000 1538; NIP 526-030-02-91; wysokość kapitału zakładowego wynosi 522 638 400 złotych, kapitał został w pełni opłacony.

The logo for Citi Handlowy, featuring the word "citi" in a blue sans-serif font with a red arc above the "i", followed by the word "handlowy" in a larger, bold, blue sans-serif font.