

 handlowy

czytaj Aktualności CitiService

Lipiec 2025 r. | Wydanie nr 7

Serwisy na skróty

Szybki kontakt z doradcą CitiService

 tel.: 801 24 84 24; 22 690 19 81

CitiDirect® Digital Onboarding

– zarządzanie listą osób upoważnionych do działania na rachunku

Przypominamy, że **CitiDirect Digital Onboarding** wspiera naszych klientów w procesie otwierania dodatkowego rachunku (w oparciu o *Formularz Otwarcia Rachunku*). Obecnie trwa faza 1, w ramach której bank częściowo wypełnia formularz, korzystając z posiadanych danych, a następnie przesyła go Państwu do uzupełnienia i podpisania. W tej fazie proces jest już cyfrowy, ale nadal inicjowany przez pracownika banku ([Kliknij i sprawdź, jak w 3 prostych krokach już wkrótce stworzysz dodatkowy rachunek >>](#)).

W docelowym modelu (faza 2) CitiDirect Digital Onboarding umożliwi Państwu samodzielnie składanie wniosków o dodatkowy rachunek, produkty bankowości transakcyjnej oraz zarządzanie listą osób upoważnionych do działania na rachunku – w dogodnym dla Państwa momencie, bezpośrednio na naszej platformie CitiDirect.

Co ważne, dzięki modułowi *Digital Signer Management* w CitiDirect (który planujemy szerzej udostępnić jeszcze w tym roku), będą mieli Państwo bezpośredni dostęp do informacji o osobach upoważnionych do działania na rachunku oraz możliwość składania online wymaganej dokumentacji w celu dodawania, zmiany lub usuwania osób upoważnionych. Bank zweryfikuje dokumenty i automatycznie zaktualizuje Centralną Bazę Osób Upoważnionych. Proces opiera się na elektronicznym obiegu dokumentów, dlatego niezwykle istotne jest, aby wszelkie zmiany były składane w ściśle określony sposób, co zagwarantuje ich szybką aktualizację.

UWAGA: aby zaktualizować listę osób upoważnionych, niezbędne jest podanie pełnych danych tych osób.

W tym celu:

- korzystaj z [Formularza Aktualizacji Osób Upoważnionych do Rachunku](#)
- podaj wszystkie wymagane ustawą AML dane wskazane na Formularzu
- wskaż indywidualne adresy służbowe e-mail osób upoważnionych (z domeną firmy)

WAŻNE: samo przekazanie do banku dokumentów rejestrowych, bez danych wskazanych powyżej, nie będzie oznaczało, że dana osoba została wskazana przez klienta do reprezentowania firmy w sprawach bankowych.

Kategorie osób upoważnionych do działania na rachunku

Reprezentanci klienta – osoby upoważnione na podstawie uchwał, pełnomocnictw, rejestrów przedsiębiorców lub innych dokumentów uprawniających do działania w imieniu klienta w celu otwierania, zamykania i prowadzenia rachunków.

Osoby upoważnione do dysponowania rachunkiem – osoby upoważnione w imieniu klienta do składania dyspozycji związanych z uznawaniem lub obciążaniem rachunku (z wyjątkiem manualnych dyspozycji przelewów). Są one również upoważnione do wydawania innych instrukcji dotyczących rachunku w zakresie realizacji usług udostępnionych przez bank, z uwzględnieniem wszelkich ograniczeń określonych obok nazwiska danej osoby.

Osoby upoważnione do podpisywania dyspozycji płatniczych w formie papierowej – osoby upoważnione do podpisywania i autoryzowania dyspozycji płatniczych składanych na formularzach papierowych, a także do ich zmiany, wycofania lub anulowania.

Osoby upoważnione do potwierdzania dyspozycji płatniczych – ze względów bezpieczeństwa bank zastrzega sobie prawo do telefonicznego potwierdzania dyspozycji. W takim przypadku bank kontaktuje się telefonicznie z jedną z osób upoważnionych w tej kategorii.

Standaryzacja i globalna spójność

Cyfrowy proces onboardingu jest zgodny z globalnym podejściem Citi, co pozwala nam zapewniać spójne doświadczenia klientów na całym świecie. W ramach tych działań wprowadzamy jednolite w Grupie Citi dokumenty określające warunki świadczenia usług, w tym: [Ogólne Warunki Prowadzenia Rachunków i Świadczenia Usług](#), [Zasady Dotyczące Poufności i Ochrony Danych Osobowych](#), [Procedury Bezpieczeństwa](#) oraz [Lokalne Warunki dla Banku Handlowego w Warszawie S.A.](#) Po podpisaniu przez Państwa [Formularza Otwarcia Rachunku](#) dokumenty te zastąpią dotychczasową dokumentację, w tym przede wszystkim Ogólne Warunki Współpracy z Klientem. Należy jednak pamiętać, że standaryzacja dokumentacji nie zmienia warunków świadczenia usług w Citi Handlowy – zapewnia jedynie spójną strukturę dokumentacyjną w całej naszej Grupie. Regulaminy dotyczące prowadzenia rachunku znajdą Państwo na naszej stronie internetowej w Strefie Klienta. Zachęcamy do zapoznania się z nimi, a w razie pytań prosimy o kontakt z Państwa Doradcą Bankowym.

Wierzymy, że opisane powyżej zmiany pozytywnie wpłyną na Państwa komfort współpracy z Citi Handlowy, zapewniając jeszcze bardziej efektywną obsługę.

Wykaz banków prowadzących rachunki nostro Banku Handlowego w Warszawie S.A

Zwracamy Waszą uwagę na aktualizację wykazu banków prowadzących rachunki nostro Banku Handlowego w Warszawie S.A. Usunięta została pozycja:

DEUTDEFF DEUTSCHE BANK AG, FRANKFURT/MAIN

WAŻNE: jedynym korespondentem dla płatności w EUR pozostaje Citibank EUROPE PLC Dublin.

UWAGA: zaleca się przesyłanie komunikatu MT103 bezpośrednio do CITIPLPX, podając w polu 53/54 komunikatu SWIFT nazwę banku korespondenta.

Waluta	SWIFT BIC	Nazwa banku korespondenta
USD	CITIUS33	CITIBANK N.A., NEW YORK
EUR	CITIE2X	CITIBANK EUROPE PLC DUBLIN
GBP	CITIGB2L	CITIBANK N.A., LONDON
CHF	CITIGB2L	CITIBANK N.A., LONDON
SEK	SWEDSESS	SWEDBANK, STOCKHOLM
DKK	NDEADKKK	NORDEA BANK DANMARK A/S, COPENHAGEN
NOK	DNBANOKK	DNB BANK ASA, OSLO
AUD	CITIAU2X	CITIBANK NA, SYDNEY
JPY	CITIJPJT	CITIBANK, N.A., TOKYO BRANCH, TOKYO
CAD	CITICATTBCH	CITIBANK, N.A., CANADIAN BRANCH, TORONTO
CZK	CITICZPX	CITIBANK EUROPE PLC, ORGANIZACNI SLOZKA, PRAGUE
HUF	CITIHUHX	CITIBANK EUROPE PLC, HUNGARIAN BRANCH, BUDAPEST
ZAR	CITIZAJX	CITIBANK N.A. SOUTH AFRICA, JOHANNESBURG
RON	CITIROBU	CITIBANK EUROPE PLC, ROMANIA BRANCH, BUCHAREST
TRY	CITITRIX	CITIBANK A.S., ISTANBUL
CNY	CITIHKHX	CITIBANK N.A., HONG KONG BRANCH, HONGKONG
BGN	CITIBGSF	CITIBANK EUROPE PLC, BULGARIA BRANCH
KZT	CITIKZKA	JSC CITIBANK KAZAKHSTAN, ALMATY
PLN	NBPLPLPW	NARODOWY BANK POLSKI, WARSZAWA
ILS	CITIILIT	CITIBANK N.A. ISRAEL

Zaktualizowana lista banków-korespondentów jest na [stronie internetowej banku >>](#)

Migracja do standardu ISO 20022 i jej wpływ na klientów Citi Handlowy w zakresie płatności SORBNET (RTGS)

Trwają prace mające na celu dostosowanie formatów komunikatów międzybankowych w związku z migracją do standardu ISO 20022. Poniżej przedstawiamy kilka istotnych kwestii, na które chcemy zwrócić Państwa uwagę.

Płatności w systemie SORBNET realizowane są z wykorzystaniem sieci SWIFT. Zgodnie z harmonogramem Narodowego Banku Polskiego, migracja do standardu ISO 20022 (komunikaty w formacie MX) nastąpi 8 września 2025 r. Poniższe zmiany wejdą w życie wraz z tą datą.

1. W ramach komunikatów MX zostanie wprowadzony nowy format międzybankowy przeznaczony do obsługi zwrotów przelewów (pacs.004). W związku z tym, na Państwa wyciągach/raportach może pojawić się nowy kod i opis transakcji dotyczący zwrotu wcześniej wykonanej płatności – **RETURNED ITEMS**.

Przykład wyciągu:

MT940	CAMT.053
:20: :25:502001024 :28:/1 :60F:C250102PLN88,88 :61:2501020102CN44,44NTRF3428200470//3428200470 /CTC/918/RETURNED ITEMS :86:/PT/FT/PY/DETALE 1 DETALE 2 DETALE 3 DETALE 4/OB /PKOPPLPW/BO/PL941030150800000004200020001/ BO1/0200020X XXXX XXXXX X/BO2/02. 00020XXXXXXX XX/XX/BO3/02-000 20XXXXXX, XXXXXX	<Acct> <Id> <Othr> <Id>502001024</Id> ... <AcctSvcrRef>3428200470</AcctSvcrRef> <BkTxCd> <Domn> <Cd>ACMT</Cd> <Fmly> <Cd>MCOP</Cd> <SubFmlyCd>OTHR</SubFmlyCd> </Fmly> </Domn> <Prtry> <Cd> 918+RETURNED ITEMS </Cd> <Issr>CITI</Issr> </Prtry> </BkTxCd> <NtryDtls> <TxDtls> <Refs>

Na ten moment zmiana ta będzie dotyczyła wyłącznie zwrotów do wychodzących płatności SORBNET (tj. przychodzących zwrotów) i będzie widoczna na wszystkich rodzajach wyciągów. Zwroty wychodzące, czyli dotyczące płatności otrzymanych na Państwa rachunek, pozostają na razie bez zmian.

Termin wdrożenia: wrzesień 2025 r.

2. Nadal będą mogli Państwo korzystać z usługi MT101 *Request for transfer* w niezmienionej formie. W przypadku podzielonej płatności (VAT Split Payment) obowiązek podawania danych w ustrukturyzowanej formie pozostaje bez zmian.

Jeśli natomiast zdecydują się Państwo już teraz na korzystanie z nowych komunikatów MX dla podzielonej płatności (VAT Split Payment), prosimy – wyjątkowo, do odwołania – o używanie komunikatu pacs.008, z zachowaniem poniższej instrukcji:

W polu *Regulatory Reporting* należy umieścić wartość „VAT53”:

```
<pacs:RgltryRptg>  
  <pacs:Dtls>  
    <pacs:Inf>VAT53</pacs:Inf>  
  </pacs:Dtls>  
</pacs:RgltryRptg>
```

W polu *Remittance information* należy, tak jak dotychczas, prawidłowo sformatować informacje towarzyszące transferowi VAT Split Payment:

/VAT/10n,2n/IDC/14x/INV/35x/TXT/33x

gdzie:

- n** – dozwolone tylko cyfry (0–9),
- x** – dowolny znak dozwolony przez SWIFT.

3. W przypadku zleceń otrzymanych komunikatem płatniczym pacs.008, nie ulegnie zmianie zasada realizacji transferów z uwzględnieniem kwoty przelewu. Płatności powyżej 1 miliona PLN zostaną wysłane systemem SORBNET, natomiast płatności poniżej 1 miliona PLN – systemem Elixir, zgodnie z wytycznymi Narodowego Banku Polskiego.

W celu realizacji płatności należy uzupełnić oba poniższe pola komunikatu MX:

```
<Dbtr> ABC PLC  
<DbtrAcct> 51103015080000000xxxxxxx
```

Termin wdrożenia: wrzesień 2025 r.

4. W ramach migracji do standardu ISO 20022 planowana jest zmiana wymogów dotyczących pól adresowych (np. adresu odbiorcy). Adres nieustrukturyzowany (czyli dane podawane ciągiem) będzie stopniowo wygaszany i zastąpi go adres ustrukturyzowany (każdy element adresu będzie miał przypisaną etykietę).

Dla płatności SORBNET w okresie przejściowym będzie można podawać adres zarówno w formie nieustrukturyzowanej, jak i ustrukturyzowanej. Nie będzie jednak możliwe zastosowanie tzw. hybrydy, czyli jednoczesnego użycia elementów adresu ustrukturyzowanego i nieustrukturyzowanego.

Przykład adresu ustrukturyzowanego:

```
<Cdtr>  
  <Nm>John Smith</Nm>  
  <PstlAdr>  
    <StrtNm>Hoogstraat</StrtNm>  
    <BldgNb>6</BldgNb>  
    <BldgNm>Premium Tower</BldgNm>  
    <Flr>18</Flr>  
    <PstlCd>1000</PstlCd>  
    <TwnNm>Brussels</TwnNm>  
    <Ctry>BE</Ctry>  
  </PstlAdr>  
</Cdtr>
```

Przykład adresu nieustrukturyzowanego:

```
<Cdtr>  
  <Nm>John Smith</Nm>  
  <PstlAdr>  
    <AdrLine>HOOGSTRAAT 6, PREMIUM</AdrLine>  
    <AdrLine>TOWER, 18TH FLOOR</AdrLine>  
    <AdrLine>1000 BRUSSELS, BELGIUM</AdrLine>  
  </PstlAdr>  
</Cdtr>
```

Okres przejściowy: wrzesień 2025 r. – listopad 2026 r. (adres ustrukturyzowany lub nieustrukturyzowany)

Termin wdrożenia: listopad 2026 r. (obowiązuje wyłącznie adres ustrukturyzowany)

5. Nowe komunikaty MX dopuszczają większą liczbę pól i znaków niż formaty MT. Bogate dane z formatów MX będą przekonwertowane do formatu MT i w takiej formie będą na razie uwzględniane na Państwa wyciągach, takich jak MT940, MT942, MT950 itp. W związku z tym może zaistnieć konieczność obciążenia danych, jeśli odebrane informacje z komunikatu MX będą bardziej obszerne, niż pozwala na to limit znaków obsługiwany w raportach/wyciągach MT.

6. W przypadku korzystania z komunikatu płatniczego pacs.009 prosimy o przestrzeganie wytycznych dotyczących płatności SORBNET.

W polu *Local instrument/Proprietary* dozwolone są tylko następujące wartości:

- DEPOZYT**
- KREDYT**
- LOKATA**
- ODSILENIE**
- PROCC**
- REZERWA**
- ZASILENIE**

Przykład:

```
<LclInstrm>  
  <Cd>  
    <Prtry>wartości w nawiasach
```

Jeśli nie zostanie użyte słowo dozwolone, płatność zostanie odrzucona.

7. W przypadku użycia komunikatu pacs.008 lub pacs.009, w celu prawidłowej realizacji płatności SORBNET, w polach Agent pośredniczący 1; Agent pośredniczący 2 ;Agent pośredniczący 3 należy wprowadzić unikalny identyfikator banku – kod **BIC**. W przeciwnym wypadku (jeśli np. zostanie wskazane imię i nazwisko oraz adres), może to spowodować nieprawidłową realizację płatności i/lub opóźnienia.

Przykład:

```
<IntrmyAgt1>  
  <FinInstnId>  
    <BIC> BIC  
  
<IntrmyAgt2>  
  <FinInstnId>  
    <BIC> BIC  
  
<IntrmyAgt3>  
  <FinInstnId>  
    <BIC> BIC
```

8. Płatności przychodzące SORBNET będą księgowane zgodnie z dyspozycją otrzymaną z banku zlecającego, również w przypadku, gdy do uznania zostanie wskazany rachunek walutowy.

Termin wdrożenia: wrzesień 2025 r.

Punkty 2-7 powyżej dotyczą płatności SORBNET inicjowanych przez Państwa przy użyciu komunikatów SWIFT.

Jednocześnie bank pracuje nad wdrożeniem formatu ISO 20022 dla wszystkich płatności i będzie informował o zmianach z odpowiednim wyprzedzeniem. Aktualne informacje znajdą Państwo na naszej [stronie internetowej >>](#)

Dodatkowo ogólne informacje dotyczące migracji w ramach ISO mogą Państwo znaleźć na globalnej stronie Citi (dostępna jest wyłącznie wersja angielska):

<https://www.citibank.com/tts/sa/iso-20022-migration/index.html>

Wyznacz Administratora Kart Business >>

by samodzielnie zarządzać programem kart business dla pracowników, bez zbędnych formalności i potrzeby kontaktu z bankiem.



Cyberbezpieczeństwo i zasady bezpiecznego korzystania z CitiDirect



Niezależnie od wielopoziomowych zabezpieczeń zastosowanych przez bank użytkownik powinien zdawać sobie sprawę z zagrożeń występujących w internecie. Zasady bezpiecznego korzystania z CitiDirect® przypominamy Państwu poniżej.

Adres logowania do systemu CitiDirect

- Wprowadzaj ręcznie w pasku adresu przeglądarki lub dodaj go do „Ulubionych”, nigdy nie wyszukuj strony logowania w wyszukiwarce internetowej.
- Upewnij się, że jesteś na właściwej stronie portalu: w oknie przeglądarki, na pasku adresu musi być widoczna zamknięta kłódka oznaczająca połączenie szyfrowane, adres strony musi zaczynać się od „https”.

Logowanie

- Korzystaj z nowoczesnego CitiDirect Mobile Token, który jest przypisany do konkretnego urządzenia, ma silne protokoły weryfikacji, mechanizmy kontroli w oparciu o czas, wbudowane parametry bezpieczeństwa. W połączeniu z uwierzytelnianiem biometrycznym CitiDirect (odciski palców lub rozpoznawanie twarzy) to wygodny i bezpieczny sposób logowania do CitiDirect.
- Sprawdź, jak włączyć CitiDirect Mobile Token dla użytkowników: [Aktywacja Przewodnik dla Administratorów Systemu >>](#). Następnie użytkownik może łatwo aktywować swój Mobile Token: [Zobacz film AKTYWACJA >>](#) i zalogować się do CitiDirect: [Zobacz film LOGOWANIE >>](#)

Dostęp i uprawnienia w CitiDirect

- Administrator ma możliwość zarządzania profilami użytkowników, ich uprawnieniami oraz narzędziami autentykacyjnymi (Mobile Token), tymczasowo blokuje wybranych użytkowników w systemie (np. w celach bezpieczeństwa). To stanowi o bezpieczeństwie środków i transakcji.
- Aby wyznaczyć Administratora, prosimy przesłać [Formularz aktywacji >>](#)

Inteligentna weryfikacja płatności

Citi® Payment Outlier Detection (CPOD) – zaawansowane narzędzie analityczne, które pomaga identyfikować transakcje różniące się istotnie od wcześniejszych trendów:

- porównuje bieżące płatności z płatnościami zrealizowanymi w przeszłości,
- pomaga identyfikować transakcje, które istotnie odstają od wcześniejszych trendów,
- wykorzystuje zaawansowane algorytmy uczenia maszynowego, które nieustannie się dostosowują i ewoluują,
- przypadki nietypowe są oznaczane do weryfikacji oraz zatwierdzenia lub odrzucenia przez wyznaczonych użytkowników przed realizacją płatności.

Citi Payment Outlier Detection jest dostępny poprzez CitiDirect bez żadnych zmian technologicznych w systemach klienta. Aby zacząć korzystać z narzędzia, skontaktuj się ze swoim Doradcą.

[Więcej informacji o CPOD >>](#)

Uważaj na złośliwe oprogramowanie rozsyłane za pomocą poczty elektronicznej

- Poczta odbiorcy weryfikuje wiadomości e-mail na podstawie adresu nadawcy. Należy pamiętać, że w przypadku wiadomości e-mail z systemu CitiDirect jest to zawsze citidirectbe.notifications@citi.com, a w przypadku CitiManagera – citicommercialcards.admin@citi.com. Wiadomości e-mail Citi Handlowy są zawsze wysyłane z domeny @citi.com.
- Citi Handlowy stosuje mechanizmy uwierzytelniania poczty elektronicznej SPF, DKIM i DMARC w celu zwiększenia bezpieczeństwa poczty elektronicznej. Jeśli Państwa firmowy serwer pocztowy jest odpowiednio skonfigurowany, złośliwa wiadomość e-mail nie zostanie dostarczona lub trafi do folderu ze spamem.
- Uwaga na załączniki: wysłane przez nas wyciągi są szyfrowane, a powiadomienia, tj. salda, zawsze będą miały zamaskowane szczegóły.

Aby dowiedzieć się więcej o niektórych typowych oszustwach, a także o najlepszych praktykach w zakresie bezpieczeństwa cybernetycznego, odwiedź stronę [Bank Handlowy w Warszawie S.A. | Citidirect - Bezpieczeństwo \(citibank.pl\)](#) lub zapisz się na darmowe szkolenie „Bezpieczeństwo w sieci” [Szkolenia | Bank Handlowy w Warszawie S.A. \(citibank.pl\)](#).

3 warstwy ochrony przeciwfraudowej – przeciwdziałaj, wykrywaj, reaguj

Istnieją trzy kluczowe kroki w opracowaniu strategicznej obrony dla Twojej organizacji. Pierwszym krokiem jest zapewnienie ochrony organizacji; drugim – zapewnienie, że w przypadku oszustwa lub próby cyberataku Twoja organizacja może szybko to wykryć, a trzecim – upewnienie się, że Twoja organizacja ma plan, jak szybko i odpowiednio **zareagować** w przypadku oszustwa lub cyberataku.

Przy opracowywaniu obrony strategicznej konieczne jest uwzględnienie trzech aspektów organizacji w każdej z powyższych faz: **ludzi, procesów i technologii**.

	LUDZIE	PROCESY	TECHNOLOGIE
 CHROŃ	- Edukuj pracowników - Ustaw kontrolę typu maker/checker	- Nadawaj tylko niezbędne dostępy i na bieżąco je przeglądaj - Usuwać pracownikom zbędne uprawnienia - Miej plan na wypadek sytuacji „high risk”	- Unikaj używania darmowych kont do obsługi korespondencji służbowej - Ogranicz pracownikom dostęp do prywatnych kont e-mail oraz serwisów społecznościowych
 WYKRYWAJ	- Zwróć uwagę na tzw. „czerwone flagi” (forma i styl maila, adres nadawcy) - Szczególną uwagę zwróć na sprawy zgłaszane w czasie wyjazdów, w piątki popołudniu czy tuż przed oficjalnymi świętami/dniami wolnymi	- Potwierdź telefonicznie każde żądanie przelewu do nowego beneficjenta - Nie oddzwaniaj na nowe lub podane jako tymczasowe numery telefonów - Upewnij się, że dzwonisz do znanej sobie osoby; unikaj dzwonienia do nowych lub nieznanych sobie osób	- Regularnie aktualizuj system antywirusowy i antymalware - Instaluj aktualizacje systemu operacyjnego i programów tak szybko, jak to możliwe - Wykorzystaj technologię oznaczania emaili jako próby phishingu
 REAGUJ	- Wyślij ostrzeżenie/alert do osób, które wiedzą, co zrobić w przypadku takich incydentów - Nie bój się używać słowa „fraud” lub „problem” - Działaj szybko; liczy się każda minuta w procesie zatrzymania i odzyskania środków	- Stwórz proces, zanim będziesz go potrzebować - Określ role i odpowiedzialności osób - Ustal, kto musi być poinformowany, co musi widzieć i kiedy - Uważnie zweryfikuj transakcje na pozostałych rachunkach, aby upewnić się, czy nie ma innych podejrzanych operacji	- Zachowaj wszystkie możliwe ślady, włączając komputery - Zaangażuj eksperta ds. bezpieczeństwa, aby sprawdzić, jak doszło do incydentu oraz ocenić podatność na kolejne ataki - Rozważ wykonanie testu podatności na kolejne ataki – zaangażuj swój dział IT, aby wysłał fałszywe e-maile typu „phishing” do pracowników

Wykorzystaj się narzędzi CitiDirect:

- Mianuj Administratora Systemu
- Zawsze wykorzystuj schemat dwuosobowy do przelewów
- Rozważ wprowadzenie limitów kwotowych lub ograniczeń godzin pracy w systemie

Święta walut: lipiec i sierpień 2025 r.

Prezentujemy Państwu dni w **lipcu i sierpniu 2025 r.**, w których dokonane zlecenia będą realizowane następnego dnia roboczego ze względu na dni wolne od pracy w danym kraju.

LIPIEC	
1	CAD
4	USD
7	KZT
14	UAH
15	TRY, UAH
21	JPY

SIERPIEŃ	
1	CHF
4	AUD, CAD
11	JPY
15	RON, PLN
20	HUF
25	GBP, UAH