

## WYTYCZNE

## WYTYCZNE EUROPEJSKIEGO BANKU CENTRALNEGO

z dnia 15 września 2010 r.

zmieniające wytyczne EBC/2007/2 w sprawie transeuropejskiego zautomatyzowanego błyskawicznego systemu rozrachunku brutto w czasie rzeczywistym (TARGET2)

(EBC/2010/12)

(2010/593/UE)

RADA PREZESÓW EUROPEJSKIEGO BANKU CENTRALNEGO,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 127 ust. 2,

uwzględniając Statut Europejskiego Systemu Banków Centralnych i Europejskiego Banku Centralnego, w szczególności jego art. 3 ust. 1 oraz art. 17, 18 i 22,

a także mając na uwadze, co następuje:

(1) Rada Prezesów Europejskiego Banku Centralnego (EBC) przyjęła wytyczne EBC/2007/2 z dnia 26 kwietnia 2007 r. w sprawie transeuropejskiego zautomatyzowanego błyskawicznego systemu rozrachunku brutto w czasie rzeczywistym (TARGET2) <sup>(1)</sup> regulujące działanie systemu TARGET2, który charakteryzuje się pojedynczą platformą techniczną zwaną jednolitą wspólną platformą (*Single Shared Platform*, SSP).

(2) W wytycznych EBC/2007/2 należy wprowadzić zmiany: a) uwzględniające aktualizacje wersji 4.0 systemu TARGET2, w szczególności mające na celu umożliwienie uczestnikom dostępu do jednego lub większej ilości rachunków w PM przez Internet; oraz b) odzwierciedlające szereg zmian technicznych spowodowanych wejściem w życie Traktatu o funkcjonowaniu Unii Europejskiej oraz wyjaśniające niektóre zagadnienia,

PRZYJMUJE NINIEJSZE WYTYCZNE:

## Artykuł 1

W wytycznych EBC/2007/2 wprowadza się następujące zmiany:

1) art. 1 ust. 1 otrzymuje brzmienie:

„1. TARGET2 umożliwia rozrachunek brutto w czasie rzeczywistym płatności w euro, przeprowadzany

w pieniądzu banku centralnego. System ten został stworzony i funkcjonuje w oparciu o SSP, za pośrednictwem której na tych samych zasadach technicznych następuje składanie i przetwarzanie wszystkich zleceń płatniczych oraz otrzymywanie płatności.”;

2) w art. 2 wprowadza się następujące zmiany:

a) następujące definicje otrzymują brzmienie:

„— »uczestniczący KBC« – krajowy bank centralny (KBC) państwa członkowskiego, którego walutą jest euro,”;

„— »adresowalny posiadacz BIC« – podmiot, który: a) posiada BIC; b) nie jest zarejestrowany jako uczestnik pośredni; oraz c) jest korespondentem lub klientem uczestnika bezpośredniego bądź też oddziałem uczestnika bezpośredniego lub uczestnika pośredniego, mającym możliwość składania zleceń płatniczych do systemu będącego komponentem TARGET2 oraz otrzymywania płatności z tego systemu za pośrednictwem uczestnika bezpośredniego,”;

b) definicja „— »bankowy kod identyfikacyjny« lub »BIC« (Bank Identifier Code) – kod zdefiniowany w normie ISO nr 9362,” otrzymuje brzmienie: „— »kod identyfikacyjny jednostki« lub »BIC« (Business Identifier Code) – kod zdefiniowany w normie ISO nr 9362,”;

c) dodaje się następujące definicje:

„— »dostęp przez Internet« – wybór przez uczestnika rachunku w PM dostępnego jedynie przez Internet, przy czym uczestnik przekazuje komunikaty płatnicze albo komunikaty kontrolne do systemu TARGET2 za pośrednictwem Internetu,”;

<sup>(1)</sup> Dz.U. L 237 z 8.9.2007, s. 1.

„— »organy certyfikacyjne« – jeden lub większą liczbę KBC wyznaczonych jako takie przez Radę Prezesów do podejmowania w imieniu Eurosystemu działań w zakresie wydawania, cofania i odnawiania certyfikatów elektronicznych oraz zarządzania tymi certyfikatami,”

„— »certyfikaty elektroniczne« albo »certyfikaty« – wydany przez organ certyfikacyjny elektroniczny plik łączący klucz publiczny z tożsamością, używany w następujących celach: dla weryfikacji, że klucz publiczny należy do określonej osoby, dla potwierdzenia tożsamości posiadacza, dla sprawdzenia podpisu tej osoby albo dla zaszyfrowania komunikatu adresowanego do tej osoby. Certyfikaty przechowuje się na fizycznie istniejącym urządzeniu, takim jak karta chipowa albo pamięć USB, przy czym ilekroć mowa jest o certyfikatach, rozumie się przez to również takie fizycznie istniejące urządzenia. Certyfikaty pełnią zasadniczą rolę w procesie identyfikacji użytkowników uzyskujących dostęp do systemu TARGET2 przez Internet i przekazujących komunikaty płatnicze albo kontrolne,”

„— »posiadacz certyfikatu« – osobę określoną z imienia i nazwiska, zidentyfikowaną i wskazaną przez uczestnika systemu TARGET2 jako uprawnioną do dostępu przez Internet do rachunku uczestnika w systemie TARGET2. Wniosek uczestnika o certyfikaty podlega weryfikacji przez KBC państwa, w którym ma siedzibę uczestnik, oraz przekazaniu organom certyfikacyjnym, które z kolei wydają certyfikaty wiążące klucz publiczny z danymi potwierdzającymi tożsamość uczestnika,”

„— »zharmonizowane warunki« – warunki określone w załącznikach II i V,”;

3) art. 6 ust. 1 i 2 otrzymuje brzmienie:

„1. Uczestniczące KBC przyjmują postanowienia wprowadzające zharmonizowane warunki uczestnictwa w TARGET2 określone w załączniku II oraz uzupełniające i zmodyfikowane zharmonizowane warunki uczestnictwa w TARGET2 z wykorzystaniem dostępu przez Internet określone w załączniku V. Postanowienia te regulują w sposób wyłączny stosunki pomiędzy danym uczestniczącym KBC a jego uczestnikami w zakresie przetwarzania płatności w PM. Dostęp do rachunku w PM można uzyskać, korzystając z dostępu przez Internet albo za pośrednictwem dostawcy usług sieciowych. Powyższe dwa sposoby dostępu do rachunku w PM wzajemnie się wykluczają; uczestnik może jednakże zdecydować się na posiadanie większej liczby rachunków w PM, z których każdy będzie dostępny albo przez Internet, albo za pośrednictwem dostawcy usług sieciowych.

2. EBC przyjmuje warunki uczestnictwa w systemie TARGET2-ECB, dokonując implementacji załącznika II, z zastrzeżeniem, iż dostęp do systemu TARGET2-ECB jest ograniczony do organizacji rozliczeniowo-rozrachunkowych, w tym podmiotów z siedzibą poza EOG, o ile podlegają one nadzorowi systemowemu właściwego organu i na ich dostęp do TARGET2-ECB wyraziła zgodę Rada Prezesów.”;

4) art. 8 ust. 1 otrzymuje brzmienie:

„1. BC Eurosystemu świadczą na rzecz systemów zewnętrznych usługi przelewu środków w pieniądzu banku centralnego w PM, z dostępem za pośrednictwem dostawcy usług sieciowych lub, o ile ma to zastosowanie w czasie okresu przejściowego, na rachunkach typu home. Usługi takie podlegają porozumieniom dwustronnym między BC Eurosystemu a danymi systemami zewnętrznymi.”;

5) art. 10 ust. 1 otrzymuje brzmienie:

„1. Rada Prezesów określa zasady i wymagania dotyczące bezpieczeństwa oraz narzędzia kontroli dla SSP oraz – podczas okresu przejściowego – dla infrastruktury technicznej rachunku typu home. Rada Prezesów określa ponadto zasady mające zastosowanie do bezpieczeństwa certyfikatów używanych przy dostępie przez Internet.”;

6) art. 16 ust. 2 otrzymuje brzmienie:

„2. Uczestniczące KBC przesyłają do EBC do dnia 31 lipca 2007 r. albo w terminie określonym przez Radę Prezesów projekty aktów prawnych, za pomocą których zamierzają zastosować się do niniejszych wytycznych.”;

7) załączniki do wytycznych EBC/2007/2 podlegają zmianom zgodnie z załącznikiem I do niniejszych wytycznych.

8) do wytycznych EBC/2007/2 dodaje się załącznik V zgodnie z załącznikiem II do niniejszych wytycznych.

Artykuł 2

### Wejście w życie

Niniejsze wytyczne wchodzi w życie dwa dni po ich przyjęciu. Niniejsze wytyczne stosuje się od dnia 22 listopada 2010 r.

*Artykuł 3***Adresaci i środki wykonawcze**

1. Niniejsze wytyczne są adresowane do wszystkich banków centralnych Eurosystemu.
2. Uczestniczące KBC przesyłają do EBC do dnia 7 października 2010 r. projekty aktów prawnych, za pomocą których zamierzają zastosować się do niniejszych wytycznych.

Sporządzono we Frankfurcie nad Menem dnia 15 września 2010 r.

*W imieniu Rady Prezesów EBC*

Jean-Claude TRICHET

Prezes EBC

---

## ZAŁĄCZNIK I

1. W załączniku I do wytycznych EBC/2007/2 wprowadza się następujące zmiany:

W załączniku I punkt 7 tabeli otrzymuje brzmienie:

„7. Obsługa		
— Zarządzanie poważnymi sytuacjami kryzysowymi	— Zarządzanie w zakresie obowiązków właściciela systemu	— Zarządzanie systemem na podstawie umowy, o której mowa w art. 5 ust. 6 niniejszych wytycznych”
— Udzielanie pozwolenia na utworzenie i działanie symulatora TARGET2	— Utrzymywanie kontaktu z użytkownikami na poziomie europejskim (z zastrzeżeniem, iż obowiązki w zakresie kontaktów biznesowych z klientami obciążają wyłącznie BC Eurosystemu) oraz monitorowanie bieżącej aktywności użytkowników z perspektywy biznesowej (zadanie BC Eurosystemu)	
— Wyznaczanie organów certyfikacyjnych dla dostępu przez Internet	— Monitorowanie rozwoju sytuacji na rynku	
— Określanie zasad i wymagań dotyczących bezpieczeństwa oraz narzędzi kontroli dla SSP	— Budżetowanie, finansowanie, fakturowanie (zadanie BC Eurosystemu) i inne zadania administracyjne	
— Określanie zasad mających zastosowanie do bezpieczeństwa certyfikatów używanych przy dostępie przez Internet		

2. W załączniku II do wytycznych EBC/2007/2 wprowadza się następujące zmiany:

1) w art. 1 wprowadza się następujące zmiany:

a) następujące definicje otrzymują brzmienie:

„— »adresowalny posiadacz BIC« (*addressable BIC holder*) – podmiot, który: a) posiada BIC; b) nie jest zarejestrowany jako uczestnik pośredni; oraz c) jest korespondentem lub klientem uczestnika bezpośredniego bądź też oddziałem uczestnika bezpośredniego lub uczestnika pośredniego, mającym możliwość składania zleceń płatniczych do systemu będącego komponentem TARGET2 oraz otrzymywania płatności z tego systemu za pośrednictwem uczestnika bezpośredniego,”

„— »instytucja kredytowa« (*credit institution*) – a) instytucję kredytową w rozumieniu [przepisy krajowe implementujące art. 4 ust. 1 lit. a) oraz, o ile ma zastosowanie, art. 2 dyrektywy bankowej], podlegającą nadzorowi właściwego organu; albo b) inną instytucję kredytową w rozumieniu art. 123 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej, podlegającą kontroli o standardzie porównywalnym do nadzoru prowadzonego przez właściwy organ.”

„— »podmiot sektora publicznego« (*public sector body*) – podmiot wchodzący w skład »sektora publicznego« rozumianego zgodnie z definicją zawartą w art. 3 rozporządzenia Rady (WE) nr 3603/93 z dnia 13 grudnia 1993 r. określającego definicje w celu zastosowania zakazów określonych w art. 104 i 104b ust. 1 Traktatu (\*),

(\*) Dz.U. L 332 z 31.12.1993, s. 1.”;

b) definicja „— »BIC« (Bankowy Kod Identyfikacyjny, *Bank Identifier Code, BIC*) – kod zdefiniowany w normie ISO nr 9362,” otrzymuje brzmienie: „— »kod identyfikacyjny jednostki« lub »BIC« (*Business Identifier Code*) – kod zdefiniowany w normie ISO nr 9362,”;

c) dodaje się następującą definicję:

„— »szczegółowa specyfikacja funkcjonalna użytkownika« albo »specyfikacja UDFS« (*User Detailed Functional Specifications, UDFS*) – najbardziej aktualną wersję specyfikacji UDFS, która jest techniczną dokumentacją określającą szczegóły współdziałania uczestnika z systemem TARGET2.”;

2) w art. 4 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Następujące typy podmiotów są uprawnione do uczestnictwa bezpośredniego w TARGET2-[oznaczenie BC/kraju]:

- a) instytucje kredytowe mające siedzibę w EOG, również jeżeli działają one za pośrednictwem oddziału mającego siedzibę w EOG;
- b) instytucje kredytowe mające siedzibę poza EOG, o ile działają one za pośrednictwem oddziału mającego siedzibę w EOG; oraz
- c) KBC państw członkowskich UE oraz EBC;

o ile podmioty, o których mowa w lit. a) i b), nie podlegają środkom ograniczającym przyjętym przez Radę Unii Europejskiej lub państwa członkowskie zgodnie z art. 65 ust. 1 lit. b), art. 75 lub art. 215 Traktatu o funkcjonowaniu Unii Europejskiej, których wprowadzenie zdaniem [oznaczenie BC/kraju], po poinformowaniu EBC, nie da się pogodzić ze sprawnym funkcjonowaniem systemu TARGET2.”;

- b) w art. 4 ust. 2 lit. e) użyte w różnych przypadkach określenia „Wspólnota Europejska” oraz „Wspólnota” zastępuje się użytym w tych samych przypadkach określeniem „Unia”;

3) art. 32 ust. 4 otrzymuje brzmienie:

„4. [Nazwa BC] przechowuje pełne dane dotyczące zleceń płatniczych złożonych przez uczestników i otrzymanych przez nich płatności przez okres [okres zgodny z wymogami właściwego prawa krajowego] od chwili złożenia takich zleceń lub otrzymania płatności, z zastrzeżeniem, że takie pełne dane będą obejmować okres co najmniej pięciu lat dla każdego uczestnika TARGET2, wobec którego zachowywana jest stała czujność na podstawie środków ograniczających przyjętych przez Radę Unii Europejskiej lub państwa członkowskie, lub dłuższy okres, o ile wymagany jest przez przepisy szczególne.”;

4) w art. 34 ust. 2 wprowadza się następujące zmiany:

- a) pod lit. d) skreśla się słowo „lub”, które dodaje się po tekście pod lit. e);
- b) dodaje się lit. f) w brzmieniu:

„f) KBC zawieszają dostęp uczestnika do kredytu w ciągu dnia albo pozbawi go takiego dostępu zgodnie z pkt 12 załącznika III.”;

5) w art. 38 ust. 2 określenie „Wspólnota” zastępuje się użytym w odpowiednim przypadku określeniem „Unia”;

6) art. 39 ust. 1 otrzymuje brzmienie:

„1. Przyjmuje się, że uczestnicy są świadomi wszystkich obowiązków ciążyących na nich w związku z przepisami o ochronie danych, o zapobieganiu praniu pieniędzy i finansowaniu terroryzmu, działalności łączącej się z ryzykiem rozprzestrzeniania broni jądrowej oraz rozwoju środków przenoszenia broni jądrowej i są oni obowiązani do ich spełniania, w szczególności poprzez podejmowanie odpowiednich środków dotyczących płatności obciążających lub uznających ich rachunki w PM. Uczestnicy są ponadto obowiązani do zaznajomienia się z zasadami przechowywania danych stosowanymi przez dostawcę usług sieciowych przed nawiązaniem stosunku umownego z dostawcą usług sieciowych.”;

7) w art. 40 ust. 1 określenie „SWIFT” zastępuje się określeniem „BIC”;

8) art. 44 ust. 2 otrzymuje brzmienie:

„2. Z zastrzeżeniem właściwości Trybunału Sprawiedliwości Unii Europejskiej, wszelkie spory wynikające ze spraw związanych ze stosunkiem, o którym mowa w ust. 1, podlegają wyłącznej jurysdykcji właściwych sądów [miejsce siedziby BC].”;

9) w dodatku I ostatnie trzy wiersze tabeli w pkt 2 ust. 1 otrzymują brzmienie:

„MT 900	Opcjonalny	Potwierdzenie obciążenia/Zmiana linii kredytowej
MT 910	Opcjonalny	Potwierdzenie uznania/Zmiana linii kredytowej
MT 940/950	Opcjonalny	Komunikat zawierający wyciąg z rachunku (klienta)”

10) w dodatku V ostatni wiersz tabeli w pkt 3 otrzymuje brzmienie:

„1.00 - 7.00	Procedura rozrachunku nocnych operacji systemów zewnętrznych (tylko dla procedury rozrachunkowej 6 dla systemów zewnętrznych)”
--------------	--

3. W załączniku III do wytycznych EBC/2007/2 wprowadza się następujące zmiany:

1) następujące definicje otrzymują brzmienie:

„— »instytucja kredytowa« – a) instytucję kredytową w rozumieniu przepisów krajowych implementujących art. 2 oraz art. 4 ust. 1 lit. a) dyrektywy bankowej podlegającą nadzorowi właściwego organu; lub b) inną instytucję kredytową w rozumieniu art. 123 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej, podlegającą kontroli o standardzie porównywalnym do nadzoru prowadzonego przez właściwy organ,”

„— »podmiot sektora publicznego« – podmiot wchodzący w skład »sektora publicznego« rozumianego zgodnie z definicją zawartą w art. 3 rozporządzenia Rady (WE) nr 3603/93 z dnia 13 grudnia 1993 r. określającego definicje w celu zastosowania zakazów określonych w art. 104 i 104b ust. 1 Traktatu (\*),

(\*) Dz.U. L 332 z 31.12.1993, s. 1.”,

„— »niewykonanie zobowiązania« – zaistnienie lub groźbę zaistnienia zdarzenia mogącego zagrozić wykonaniu zobowiązań podjętych przez dany podmiot na podstawie krajowych postanowień stanowiących implementację niniejszych wytycznych lub na podstawie innych zasad (w tym określonych przez Radę Prezesów w odniesieniu do operacji polityki pieniężnej Eurosystemu) mających zastosowanie do stosunku między tym podmiotem a którymkolwiek z BC Eurosystemu, w tym w szczególności:

- a) przypadek, gdy podmiot przestaje spełniać kryteria dostępu lub wymagania określone w załączniku II oraz, o ile ma on zastosowanie, w załączniku V;
- b) wszczęcie postępowania upadłościowego w stosunku do podmiotu;
- c) złożenie wniosku o wszczęcie postępowania wskazanego w lit. b);
- d) wydanie przez podmiot pisemnego oświadczenia o niemożności spłaty całości lub części zadłużenia lub wykonania zobowiązań związanych z kredytem w ciągu dnia;
- e) zawarcie przez podmiot układu lub ugody z wierzycielami;
- f) sytuacja, w której podmiot jest niewypłacalny lub niezdolny do spłaty swoich długów, albo zostanie uznany za taki przez odpowiedni uczestniczący KBC;
- g) sytuacja, w której saldo dodatnie podmiotu na jego rachunku w PM, względnie całość lub znacząca część aktywów podmiotu zostają objęte środkiem zabezpieczającym, względnie podlegają zajęciu, egzekucji lub jakimkolwiek innemu postępowaniu zmierzającemu do ochrony interesu publicznego lub praw wierzycieli podmiotu;
- h) sytuacja, w której uczestnictwo danego podmiotu w systemie będącym komponentem systemu TARGET2 lub w systemie zewnętrznym zostaje zawieszona lub ustaje;
- i) sytuacja, w której jakiegokolwiek istotne wystąpienie albo oświadczenie złożone przez podmiot przed zawarciem umowy, lub wystąpienie albo oświadczenie, co do którego – zgodnie z prawem właściwym – przyjmuje się, że zostało złożone przez podmiot, okaże się nieprawidłowe lub nieprawdziwe; lub
- j) dokonanie przelewu (cesji) całości lub znaczącej części aktywów podmiotu.”;

2) pkt 1 otrzymuje brzmienie:

„1. Uczestniczące KBC udzielają kredytu w ciągu dnia podmiotom, o których mowa w ust. 2, posiadającym rachunek w danym uczestniczącym KBC, o ile podmioty te nie podlegają środkom ograniczającym przyjętym przez Radę Unii Europejskiej lub państwa członkowskie zgodnie z art. 65 ust. 1 lit. b), art. 75 lub art. 215 Traktatu o funkcjonowaniu Unii Europejskiej, których wprowadzenie zdaniem [oznaczenie BC/kraju], po poinformowaniu EBC, nie da się pogodzić ze sprawnym funkcjonowaniem systemu TARGET2. Kredytu w ciągu dnia nie udziela się jednakże podmiotowi mającemu siedzibę w kraju niebędącym państwem członkowskim siedziby uczestniczącego KBC, w którym podmiot ten posiada rachunek.”;

## 3) pkt 4 otrzymuje brzmienie:

„4. Kredytu w ciągu dnia udziela się za kwalifikowanym zabezpieczeniem, w formie zabezpieczonych śróddziennych przekroczeń salda lub śróddziennych transakcji z przyrzeczeniem odkupu, z zachowaniem postanowień dodatkowych minimalnych cech wspólnych (w tym postanowień dotyczących wymienionych w nich zdarzeń niewykonania zobowiązania oraz ich skutków) ustalanych przez Radę Prezesów w odniesieniu do operacji polityki pieniężnej Eurosystemu. Kwalifikowane zabezpieczenie składa się z aktywów i instrumentów tego samego rodzaju, co aktywa kwalifikowane do wykorzystania w operacjach polityki pieniężnej Eurosystemu, oraz podlega tym samym zasadom wyceny i kontroli ryzyka, co zasady określone w załączniku I do wytycznych EBC/2000/7.”;

## 4) pkt 12 otrzymuje brzmienie:

„12. a) Uczestniczący KBC może zawiesić dostęp do kredytu w ciągu dnia lub pozbawić takiego dostępu w przypadku zaistnienia jednego z następujących zdarzeń niewykonania zobowiązania:

- (i) rachunek podmiotu w uczestniczącym KBC zostanie zawieszony lub zamknięty;
- (ii) dany podmiot przestanie spełniać którekolwiek z określonych w niniejszym załączniku wymagań uzyskania dostępu do kredytu w ciągu dnia;
- (iii) właściwy organ sądowy lub inny właściwy organ postanowi o wszczęciu w stosunku do danego podmiotu postępowania mającego na celu jego likwidację; zostanie powołany dla podmiotu likwidator lub podobny organ, lub wszczęte inne podobne postępowanie;
- (iv) podmiot zostanie objęty blokadą środków finansowych lub innymi podjętymi przez Unię środkami skutkującymi ograniczeniem zdolności podmiotu do korzystania ze swoich środków; lub

b) uczestniczący KBC może zawiesić dostęp do kredytu w ciągu dnia lub pozbawić takiego dostępu w przypadku, gdy KBC zawiesi lub wypowie uczestnictwo uczestnika w TARGET2 zgodnie z art. 34 ust. 2 lit. b)–e) załącznika II lub w razie wystąpienia jednego lub większej liczby zdarzeń niewykonania zobowiązania (innych niż te, o których mowa w art. 34 ust. 2 lit. a); lub

c) jeżeli Eurosystem zawiesi, ograniczy lub wykluczy dostęp kontrahentów do instrumentów polityki pieniężnej ze względu na wymogi ostrożności lub w inny sposób zgodny z punktem 2.4 załącznika I do wytycznych EBC/2000/7, uczestniczące KBC wykonają odpowiednio powyższe zawieszenie, ograniczenie lub wykluczenie w odniesieniu do dostępu do kredytu w ciągu dnia, zgodnie z postanowieniami umownymi lub normatywnymi stosowanymi przez właściwy KBC.”.

## 4. W załączniku IV do wytycznych EBC/2007/2 wprowadza się następujące zmiany:

## 1) pkt 9 ust. 4 otrzymuje brzmienie:

„4. Banki rozrachunkowe i systemy zewnętrzne mają dostęp do informacji za pośrednictwem ICM. Systemy zewnętrzne są powiadamiane o dokonaniu rozrachunku albo jego niedośściu do skutku. Jeśli system zewnętrzny inicjuje przekazanie płynności z rachunku lustrzanego na rachunek w PM banku rozrachunkowego, wówczas banki rozrachunkowe mające dostęp do TARGET2 za pośrednictwem dostawcy usług sieciowych zostają powiadomione o dokonaniu uznania za pomocą komunikatu SWIFT MT 202. Uczestnicy korzystający z dostępu przez Internet są powiadamiani komunikatem w ICM.”;

## 2) pkt 10 ust. 4 otrzymuje brzmienie:

„4. Banki rozrachunkowe i systemy zewnętrzne mają dostęp do informacji za pośrednictwem ICM. Systemy zewnętrzne są powiadamiane komunikatem w ICM o dokonaniu rozrachunku albo jego niedośściu do skutku. Jeżeli zgłoszą one takie żądanie, banki rozrachunkowe mające dostęp do TARGET2 za pośrednictwem dostawcy usług sieciowych są powiadamiane o skutecznym dokonaniu rozrachunku za pomocą komunikatu SWIFT MT 900 albo MT 910. Uczestnicy korzystający z dostępu przez Internet są powiadamiani komunikatem w ICM.”;

## 3) pkt 11 ust. 5 otrzymuje brzmienie:

„5. Banki rozrachunkowe i systemy zewnętrzne mają dostęp do informacji za pośrednictwem ICM. Systemy zewnętrzne są powiadamiane o dokonaniu rozrachunku albo jego niedośściu do skutku w oparciu o wybraną opcję – zawiadomienie pojedyncze lub globalne. Jeżeli zgłoszą one takie żądanie, banki rozrachunkowe są powiadamiane o skutecznym dokonaniu rozrachunku za pomocą komunikatu SWIFT MT 900 albo MT 910. Uczestnicy korzystający z dostępu przez Internet są powiadamiani komunikatem w ICM.”;

4) pkt 12 ust. 9 otrzymuje brzmienie:

„9. Banki rozrachunkowe i systemy zewnętrzne mają dostęp do informacji za pośrednictwem ICM. Systemy zewnętrzne są powiadamiane o dokonaniu rozrachunku albo jego niedojściu do skutku. Jeżeli zgłoszą one takie żądanie, banki rozrachunkowe są powiadamiane o skutecznym dokonaniu rozrachunku za pomocą komunikatu SWIFT MT 900 albo MT 910. Uczestnicy korzystający z dostępu przez Internet są powiadamiani komunikatem w ICM.”;

5) pkt 13 ust. 3 otrzymuje brzmienie:

„3. Banki rozrachunkowe i systemy zewnętrzne mają dostęp do informacji za pośrednictwem ICM. Systemy zewnętrzne są powiadamiane o dokonaniu rozrachunku albo jego niedojściu do skutku. Jeżeli zgłoszą one takie żądanie, banki rozrachunkowe są powiadamiane o skutecznym dokonaniu rozrachunku za pomocą komunikatu SWIFT MT 900 albo MT 910. Uczestnicy korzystający z dostępu przez Internet są powiadamiani komunikatem w ICM.”;

6) pkt 14 ust. 2 otrzymuje brzmienie:

„2. W razie zgłoszenia takiego żądania, banki rozrachunkowe są powiadamiane za pomocą komunikatu SWIFT MT 900 albo MT 910, a uczestnicy korzystający z dostępu przez Internet za pomocą komunikatu w ICM o uznaniu i obciążeniu ich rachunków w PM, oraz, o ile są one prowadzone, ich subkont.”;

7) pkt 14 ust. 7 lit. c) otrzymuje brzmienie:

„c) zlecenia SWIFT przekazane w formie komunikatu MT 202 albo wynikające z automatycznego odzwierciedlenia zawartości ekranów na komunikat MT 202 dla użytkowników korzystających z dostępu przez Internet, które mogą być składane wyłącznie w czasie trwania procedury rozrachunkowej 6 i tylko podczas przetwarzania dziennego. Takie zlecenia podlegają natychmiastowemu rozrachunkowi.”;

8) w pkt 14 ust. 12 akapit drugi otrzymuje brzmienie:

„System zewnętrzny inicjujący instrukcję płatniczą oraz drugi wspomniany system zewnętrzny powiadamia się o zakończeniu rozrachunku. Jeżeli zgłoszą one takie żądanie, banki rozrachunkowe powiadamia się o skutecznym dokonaniu rozrachunku za pomocą komunikatu SWIFT MT 900 albo MT 910. Uczestnicy korzystający z dostępu przez Internet są powiadamiani komunikatem w ICM.”;

9) w pkt 14 ust. 13 drugi akapit otrzymuje brzmienie:

„System zewnętrzny inicjujący instrukcję płatniczą oraz drugi wspomniany system zewnętrzny powiadamia się o zakończeniu rozrachunku. Jeżeli zgłoszą one takie żądanie, banki rozrachunkowe powiadamia się o skutecznym dokonaniu rozrachunku za pomocą komunikatu SWIFT MT 900 albo MT 910. Uczestnicy korzystający z dostępu przez Internet są powiadamiani komunikatem w ICM.”;

10) w pkt 14 ust. 17 drugi akapit otrzymuje brzmienie:

„System zewnętrzny inicjujący instrukcję płatniczą oraz drugi wspomniany system zewnętrzny powiadamia się o zakończeniu rozrachunku. Jeżeli zgłoszą one takie żądanie, banki rozrachunkowe powiadamia się o skutecznym dokonaniu rozrachunku za pomocą komunikatu SWIFT MT 900 albo MT 910. Uczestnicy korzystający z dostępu przez Internet są powiadamiani komunikatem w ICM.”;

11) w pkt 14 ust. 18 drugi akapit otrzymuje brzmienie:

„System zewnętrzny inicjujący instrukcję płatniczą oraz drugi wspomniany system zewnętrzny powiadamia się o zakończeniu rozrachunku. Jeżeli zgłoszą one takie żądanie, banki rozrachunkowe powiadamia się o skutecznym dokonaniu rozrachunku za pomocą komunikatu SWIFT MT 900 albo MT 910. Uczestnicy korzystający z dostępu przez Internet są powiadamiani komunikatem w ICM.”.



## ZAŁĄCZNIK II

Dodaje się załącznik V w brzmieniu:

## „ZAŁĄCZNIK V

**UZUPEŁNIAJĄCE I ZMODYFIKOWANE ZHARMONIZOWANE WARUNKI UCZESTNICTWA W TARGET2 Z WYKORZYSTANIEM DOSTĘPU PRZEZ INTERNET**

## Artykuł 1

**Zakres regulacji**

Do uczestników korzystających z dostępu przez Internet do jednego albo większej liczby rachunków w PM stosuje się warunki określone w załączniku II z zastrzeżeniem postanowień niniejszego załącznika.

## Artykuł 2

**Definicje**

Dla celów niniejszego załącznika, w uzupełnieniu definicji zawartych w załączniku II, stosuje się następujące definicje:

- »organy certyfikacyjne« – jeden lub większa liczba KBC wyznaczonych jako takie przez Radę Prezesów do podejmowania w imieniu Eurosystemu działań w zakresie wydawania, cofania i odnawiania certyfikatów elektronicznych oraz zarządzania tymi certyfikatami,
- »certyfikaty elektroniczne« albo »certyfikaty« – wydany przez organy certyfikacyjne elektroniczny plik łączący klucz publiczny z tożsamością, używany w następujących celach: dla weryfikacji, że klucz publiczny należy do określonej osoby, dla potwierdzenia tożsamości posiadacza, dla sprawdzenia podpisu tej osoby albo dla zaszyfrowania komunikatu adresowanego do tej osoby. Certyfikaty przechowuje się na fizycznie istniejącym urządzeniu, takim jak karta chipowa albo pamięć USB, przy czym ilekroć mowa jest o certyfikatach, rozumie się przez to również takie fizycznie istniejące urządzenia. Certyfikaty pełnią zasadniczą rolę w procesie identyfikacji użytkowników uzyskujących dostęp do systemu TARGET2 przez Internet i przekazujących komunikaty płatnicze albo kontrolne,
- »posiadacz certyfikatu« – osoba określona z imienia i nazwiska, zidentyfikowana i wskazana przez uczestnika systemu TARGET2 jako uprawniona do dostępu przez Internet do rachunku uczestnika w systemie TARGET2. Wniosek uczestnika o certyfikaty podlega weryfikacji przez KBC państwa, w którym ma siedzibę uczestnik, oraz przekazaniu organom certyfikacyjnym, które z kolei wydają certyfikaty wiążące klucz publiczny z danymi potwierdzającymi tożsamość uczestnika,
- »dostęp przez Internet« – wybór przez uczestnika rachunku w PM dostępnego jedynie przez Internet, przy czym uczestnik przekazuje komunikaty płatnicze albo komunikaty kontrolne do systemu TARGET2 za pośrednictwem Internetu,
- »dostawca usług internetowych« – przedsiębiorstwo lub organizacja, tj. brama sieciowa, z której uczestnik TARGET2 korzysta w celu uzyskiwania dostępu do swojego rachunku w TARGET2 z wykorzystaniem dostępu przez Internet.

## Artykuł 3

**Przepisy niemające zastosowania**

Następujących przepisów załącznika II nie stosuje się do dostępu przez Internet:

art. 4 ust. 1 lit. c) oraz ust. 2 lit. d); art. 5 ust. 2, 3 i 4; art. 6 i 7; art. 11 ust. 8; art. 14 ust. 1 lit. a); art. 17 ust. 2; art. 23–26; art. 41 oraz dodatki I, VI i VII.

## Artykuł 4

**Postanowienia uzupełniające i zmodyfikowane**

Następujące przepisy załącznika II stosuje się do dostępu przez Internet z uwzględnieniem zmian wskazanych poniżej:

1) art. 2 ust. 1 otrzymuje brzmienie:

»1. Następujące dodatki stanowią integralną część niniejszych Warunków i są stosowane do uczestników korzystających z dostępu przez Internet do rachunku w PM:

Dodatek IA do załącznika V: Specyfikacje techniczne przetwarzania zleceń płatniczych dla dostępu przez Internet

Dodatek IIA do załącznika V: Taryfa opłat i fakturowanie dla dostępu przez Internet

Dodatek II: System rekompensat w TARGET2

Dodatek III: Ramowa treść opinii o zdolności i opinii krajowej

Dodatek IV, z wyłączeniem pkt 7 lit. b): Procedury zapewniania ciągłości działania i postępowania w sytuacjach awaryjnych

Dodatek V: Harmonogram operacyjny;

2) w art. 3 wprowadza się następujące zmiany:

a) ust. 4 otrzymuje brzmienie:

»4. Podmiotem świadczącym usługi na podstawie niniejszych Warunków jest [nazwa BC]. Działania i zaniechania BC dostarczających platformę SSP oraz organów certyfikacyjnych są uważane za działania i zaniechania [nazwa BC], za które ponosi on odpowiedzialność zgodnie z art. 31. Uczestnictwo na podstawie niniejszych Warunków nie prowadzi do powstania stosunków umownych między uczestnikami a BC dostarczającymi platformę SSP, w zakresie, w jakim działają one w tym charakterze. Instrukcje (*instructions*), komunikaty (*messages*) lub informacje otrzymywane przez uczestnika z SSP lub przesyłane przez uczestnika do SSP w związku z usługami świadczonymi na podstawie niniejszych Warunków uważa się za otrzymywane od lub wysyłane do [nazwa BC].«;

b) ust. 6 otrzymuje brzmienie:

»6. Uczestnictwo w TARGET2 następuje poprzez uczestnictwo w systemie będącym komponentem TARGET2. Niniejsze Warunki określają wzajemne prawa i obowiązki uczestników TARGET2-[oznaczenie BC/kraju] oraz [nazwa BC]. Zasady przetwarzania zleceń płatniczych (tytuł IV) odnoszą się do wszystkich zleceń płatniczych składanych lub płatności otrzymywanych przez dowolnego uczestnika TARGET2; stosuje się je z zastrzeżeniem załącznika V.«;

3) art. 4 ust. 2 lit. e) otrzymuje brzmienie:

»e) instytucje kredytowe lub którekolwiek podmioty należące do kategorii wymienionych w lit. a)–c), w obu przypadkach pod warunkiem, iż mają one siedzibę w kraju, z którym Unia zawarła porozumienie walutowe umożliwiające takim podmiotom dostęp do systemów płatności w Unii, z zastrzeżeniem warunków określonych w takim porozumieniu walutowym oraz o ile odpowiednie przepisy mające zastosowanie w takim kraju są równoważne odpowiednim przepisom unijnym.«;

4) w art. 8 wprowadza się następujące zmiany:

a) ust. 1 lit. a) ppkt (i) otrzymuje brzmienie:

»1. Dla otwarcia rachunku z dostępem przez Internet w TARGET2-[oznaczenie BC/kraju], podmiot ubiegający się o uczestnictwo jest obowiązany:

a) spełnić następujące wymagania techniczne:

(i) zapewnić instalację, zarządzanie, obsługę i kontrolowanie oraz bezpieczeństwo infrastruktury informatycznej niezbędnej do przyłączenia do TARGET2-[oznaczenie BC/kraju] oraz do składania w nim zleceń płatniczych, zgodnie ze specyfikacjami technicznymi w dodatku IA do załącznika V. Spełniając te wymagania, podmioty ubiegające się o uczestnictwo mogą korzystać z usług osób trzecich, ponosząc jednak wyłączną odpowiedzialność w tym zakresie; oraz«;

b) dodaje się ust. 1 lit. c) w brzmieniu:

»c) wyrazić wolę uzyskania dostępu do swojego rachunku w PM przez Internet, jak również złożyć wniosek o osobny rachunek w PM w systemie TARGET2, jeżeli ma zamiar uzyskania dodatkowo możliwości dostępu do TARGET2 za pośrednictwem dostawcy usług sieciowych. Podmiot ubiegający się o uczestnictwo składa należycie wypełniony formularz wniosku o wydanie certyfikatów elektronicznych koniecznych dla uzyskania dostępu przez Internet do TARGET2.«;

5) w art. 9 wprowadza się następujące zmiany:

a) ust. 3 otrzymuje brzmienie:

»3. Uczestnicy korzystający z dostępu przez Internet są uprawnieni jedynie do wglądu do TARGET2 directory przez Internet i nie mogą jej rozpowszechniać ani w ramach swojego przedsiębiorstwa, ani na zewnątrz.«;

b) ust. 5 otrzymuje brzmienie:

»5. Uczestnicy przyjmują do wiadomości, że [nazwa BC] oraz inne BC są uprawnione do publikowania nazw oraz BIC uczestników.«;

6) w art. 10 wprowadza się następujące zmiany:

a) ust. 1 i 2 otrzymują brzmienie:

»1. [Nazwa BC] oferuje dostęp przez Internet opisany w załączniku V. O ile nie zostało to odmiennie uregulowane w niniejszych Warunkach lub przepisach prawa, [nazwa BC] podejmuje w celu wykonania zobowiązań wskazanych w niniejszych Warunkach wszelkie rozsądnie wymagane działania w granicach swoich możliwości, nie ponosząc jednak odpowiedzialności za osiągnięcie pożądanego wyniku.

2. Uczestnicy korzystający z dostępu przez Internet do TARGET2 ponoszą opłaty określone w dodatku IIA do załącznika V.«;

b) dodaje się ust. 5 w brzmieniu:

»5. Uczestnicy są obowiązani do:

a) aktywnego sprawdzania, w regularnych odstępach czasu w każdym dniu operacyjnym, wszelkich informacji udostępnianych im w ICM, w szczególności pod kątem pojawienia się informacji dotyczących ważnych zdarzeń w systemie (takich jak komunikaty dotyczące rozrachunku w systemach zewnętrznych) oraz zdarzeń związanych z wykluczeniem albo zawieszeniem uczestnika. [Nazwa BC] nie ponosi odpowiedzialności za jakąkolwiek szkodę, bezpośrednią bądź pośrednią, spowodowaną zaniechaniem przez uczestnika sprawdzania powyższych informacji;

b) zapewniania ciągłego przestrzegania wymagań dotyczących bezpieczeństwa określonych w dodatku IA do załącznika V, w szczególności w zakresie przechowywania certyfikatów, oraz do stałego dochowywania zasad i procedur zapewniających, aby posiadacze certyfikatów byli świadomi odpowiedzialności w zakresie bezpiecznego przechowywania certyfikatów.«;

7) w art. 11 wprowadza się następujące zmiany:

a) dodaje się ust. 5a w brzmieniu:

»5a. Uczestnicy odpowiadają za terminowe aktualizowanie formularzy dla wydawania certyfikatów elektronicznych potrzebnych do uzyskania dostępu przez Internet do TARGET2, jak również za składanie do [nazwa BC] nowych formularzy dla wydawania takich certyfikatów elektronicznych. Uczestnicy odpowiadają również za sprawdzanie prawidłowości dotyczących ich informacji wprowadzanych do TARGET2-[oznaczenie BC/kraju] przez [nazwa BC].«;

b) ust. 6 otrzymuje brzmienie:

»6. [Nazwa BC] uważa się za upoważniony do przekazywania organom certyfikacyjnym jakichkolwiek potrzebnych tym organom informacji dotyczących uczestników.«;

8) art. 12 ust. 7 otrzymuje brzmienie:

»7. Każdemu uczestnikowi korzystającemu z tej usługi [nazwa BC] udostępnia codzienne wyciągi z rachunku.«;

9) art. 13 lit. b) otrzymuje brzmienie:

»b) instrukcje obciążenia bezpośredniego otrzymywane na podstawie upoważnienia do obciążenia bezpośredniego. Uczestnicy korzystający z dostępu przez Internet nie mają możliwości wysyłania instrukcji obciążenia bezpośredniego ze swoich rachunków w PM; oraz«;

10) art. 14 ust. 1 lit. b) otrzymuje brzmienie:

»b) komunikat płatniczy jest zgodny z zasadami formatowania oraz warunkami systemu TARGET2-[oznaczenie BC/kraju] i przejdzie test na dwukrotne wprowadzenie, zgodnie z dodatkiem IA do załącznika V; oraz«;

11) art. 16 ust. 2 otrzymuje brzmienie:

»2. Uczestnicy korzystający z dostępu przez Internet nie mogą korzystać z funkcji grupy AL w odniesieniu do swoich rachunków w PM dostępnych przez Internet, ani łączyć tych rachunków w PM dostępnych przez Internet z jakimikolwiek innymi posiadanymi przez nich rachunkami w TARGET2. Limity mogą być oznaczone jedynie w odniesieniu do grupy AL jako całości. Limity nie mogą być ustalane w odniesieniu do pojedynczego rachunku w PM uczestnika grupy AL.«;

12) art. 18 ust. 3 otrzymuje brzmienie:

»3. W przypadku posłużenia się wskaźnikiem najpóźniejszego terminu obciążenia przyjęte zlecenie płatnicze podlega zwrotowi jako niewykonane, jeżeli nie może zostać rozliczone do wskazanego terminu obciążenia. Na 15 minut przed określonym terminem obciążenia uczestnik zlecający zostaje powiadomiony przez ICM, zamiast wysyłania automatycznego zawiadomienia za pośrednictwem ICM. Uczestnik zlecający może również posłużyć się wskaźnikiem najpóźniejszego terminu obciążenia wyłącznie w charakterze ostrzegawczym. W takim przypadku dane zlecenie płatnicze nie podlega zwrotowi.«;

13) art. 21 ust. 4 otrzymuje brzmienie:

»4. Na wniosek płatnika [nazwa BC] może postanowić o dokonaniu zmiany pozycji w kolejce oczekujących zleceń płatniczych bardzo pilnego zlecenia płatniczego (z wyjątkiem bardzo pilnych zleceń płatniczych w zakresie procedury rozrachunkowej 5 i 6), o ile taka zmiana nie wpłynie na sprawny rozrachunek przez systemy zewnętrzne w TARGET2 lub w inny sposób nie zwiększy ryzyka systemowego.«;

14) w art. 28 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

»1. Obowiązkiem uczestników korzystających z dostępu przez Internet jest wdrożenie odpowiednich narzędzi kontroli w zakresie bezpieczeństwa, w szczególności określonych w dodatku IA do załącznika V, chroniących ich systemy przed nieuprawnionym dostępem i wykorzystaniem. Uczestnicy ponoszą wyłączną odpowiedzialność za odpowiednią ochronę poufności, integralności i dostępności ich systemów.«;

b) dodaje się ust. 4 w brzmieniu:

»4. Uczestnicy korzystający z dostępu przez Internet niezwłocznie informują [nazwa BC] o zdarzeniach mogących mieć wpływ na ważność certyfikatów, w szczególności zdarzeniach określonych w dodatku IA do załącznika V, w tym, bez ograniczeń, o stracie lub niewłaściwym użyciu.«;

15) art. 29 otrzymuje brzmienie:

»Artykuł 29

#### **Korzystanie z ICM**

1. ICM:

a) umożliwia uczestnikom wprowadzanie płatności;

b) umożliwia uczestnikom dostęp do informacji dotyczących ich rachunków oraz zarządzanie płynnością;

c) może być używany w celu składania zleceń przekazania płynności; oraz

d) umożliwia uczestnikom dostęp do komunikatów systemu.

2. Dalsze szczegóły techniczne dotyczące ICM w zakresie korzystania w związku z dostępem przez Internet zawiera dodatek IA do załącznika V.«;

16) w art. 32 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

»1. O ile niniejsze Warunki nie stanowią inaczej, wszystkie odnoszące się do TARGET2 komunikaty związane z płatnościami oraz przetwarzaniem płatności, takie jak potwierdzenia obciążenia i uznania, bądź też komunikaty zawierające wyciągi przesyłane między [nazwa BC] a uczestnikami, udostępnia się uczestnikowi w ICM.«;

b) ust. 3 otrzymuje brzmienie:

»3. W przypadku awarii połączenia uczestnika uczestnik korzysta z alternatywnych środków przekazu komunikatów, określonych w dodatku IA do załącznika V. W takich przypadkach zapisana lub wydrukowana wersja komunikatu przedstawiona przez [nazwa BC] jest akceptowana jako dowód.«;

17) art. 34 ust. 4 lit. c) otrzymuje brzmienie:

- »c) Po otrzymaniu przez uczestników korzystających z dostępu przez Internet powyższego komunikatu ICM są oni uważani za poinformowanych o ustaniu lub zawieszeniu uczestnictwa uczestnika w TARGET2-[oznaczenie BC/kraju] albo innym systemie będącym komponentem TARGET2. Uczestnicy ponoszą wszelkie straty wynikające ze skierowania zleceń płatniczych do uczestników, których uczestnictwo zostało zawieszono lub ustało, jeżeli dane zlecenie płatnicze zostało wprowadzone do TARGET2-[oznaczenie BC/kraju] po udostępnieniu komunikatu ICM.«;

18) art. 39 ust. 1 otrzymuje brzmienie:

- »1. Przyjmuje się, że uczestnicy są świadomi wszystkich obowiązków ciążących na nich w związku z przepisami o ochronie danych, o zapobieganiu praniu pieniędzy i finansowaniu terroryzmu, działalności łączącej się z ryzykiem rozprzestrzeniania broni jądrowej oraz rozwoju środków przenoszenia broni jądrowej i są oni obowiązani do ich spełniania, w szczególności poprzez podejmowanie odpowiednich środków dotyczących płatności obciążających lub uznających ich rachunki w PM. Przed nawiązaniem stosunku umownego z dostawcą usług internetowych uczestnicy korzystający z dostępu przez Internet są obowiązani do zaznajomienia się z zasadami przechowywania danych stosowanymi przez dostawcę usług internetowych.«;

19) art. 40 ust. 1 otrzymuje brzmienie:

- »1. O ile niniejsze Warunki nie stanowią inaczej, wszelkie zawiadomienia wymagane lub dopuszczalne zgodnie z niniejszymi Warunkami przekazuje się pocztą poleconą, faksem lub w inny sposób na piśmie. Zawiadomienia kierowane do [nazwa BC] przekazuje się dyrektorowi [departamentu systemu płatniczego lub innej odpowiedniej jednostki organizacyjnej BC] [nazwa BC], [adres BC], lub do [adres BIC BC]. Zawiadomienia kierowane do uczestnika przekazuje się na adres, numer faksu lub na jego adres BIC, zgłaszany przez uczestnika [nazwa BC] i aktualizowany.«;

20) art. 45 otrzymuje brzmienie:

»Artykuł 45

#### **Odrębność postanowień**

Jeżeli którekolwiek z postanowień niniejszych Warunków lub załącznika V jest lub stanie się nieważne, okoliczność taka nie wyklucza stosowania wszystkich pozostałych postanowień Warunków oraz załącznika V.«.

## Dodatek IA

**SPECYFIKACJE TECHNICZNE PRZETWARZANIA ZLECEŃ PŁATNICZYCH DLA DOSTĘPU PRZEZ INTERNET**

W uzupełnieniu zharmonizowanych warunków, do przetwarzania zleceń płatniczych z wykorzystaniem dostępu przez Internet stosuje się następujące zasady:

**1. Wymagania techniczne związane z uczestnictwem w systemie TARGET2-[oznaczenie BC/kraju] w zakresie infrastruktury, sieci oraz formatów**

- 1) Uczestnicy korzystający z dostępu przez Internet przyłączają się do ICM systemu TARGET2, korzystając z klienta lokalnego, systemu operacyjnego oraz przeglądarki internetowej określonych w załączniku »Uczestnictwo przez Internet – Wymagania systemowe dla dostępu przez Internet« (*Internet-based participation - System requirements for Internet access*) do Szczegółowej specyfikacji funkcjonalnej użytkownika (*User Detailed Functional Specifications, UDFS*), ze zdefiniowanymi ustawieniami. Rachunek w PM każdego z Uczestników jest identyfikowany za pomocą 8- lub 11-cyfrowego kodu BIC. Ponadto przed dopuszczeniem do uczestnictwa w systemie TARGET2-[oznaczenie BC/kraju] każdy uczestnik przechodzi serię testów potwierdzających jego przygotowanie techniczne i operacyjne.
- 2) Przy składaniu zleceń płatniczych i wymianie komunikatów płatniczych w PM korzysta się z BIC platformy TARGET2, TRGTXEPMLVP, jako nadawcy/odbiorcy komunikatu. Zlecenia płatnicze wysyłane do uczestnika korzystającego z dostępu przez Internet powinny identyfikować tego uczestnika otrzymującego w polu instytucji beneficjenta (*beneficiary institution*). Zlecenia płatnicze składane przez uczestnika korzystającego z dostępu przez Internet będą identyfikować tego uczestnika jako instytucję składającą zlecenie (*ordering institution*).
- 3) Uczestnicy korzystający z dostępu przez Internet korzystają z usług infrastruktury klucza publicznego określonych w publikacji »User Manual Internet Access for the public-key certification service« (Podręcznik użytkownika dotyczący dostępu przez Internet do usług certyfikacji klucza publicznego).

**2. Typy komunikatów płatniczych**

- 1) Uczestnicy z dostępem przez Internet mogą dokonywać następujących rodzajów płatności:
  - a) płatności klientowskie, tj. polecenia przelewu, dla których klient zlecający lub beneficjent nie są instytucjami finansowymi;
  - b) płatności klientowskie STP, tj. polecenia przelewu, dla których klient zlecający lub beneficjent nie są instytucjami finansowymi, wykonywane w trybie przetwarzania bezpośredniego;
  - c) transfery międzybankowe w celu żądania przepływu środków pomiędzy instytucjami finansowymi;
  - d) płatności pokrywające w celu żądania przepływu środków pomiędzy instytucjami finansowymi związanego z klientowskim poleceniem przelewu.

Uczestnicy korzystający z dostępu przez Internet do rachunku w PM mogą dodatkowo otrzymywać zlecenia obciążenia bezpośredniego.

- 2) Uczestnicy przestrzegają określeń pól zdefiniowanych w rozdziale 9.1.2.2 UDFS, księga 1.
- 3) Zawartość pól podlega zatwierdzeniu na poziomie systemu TARGET2-[oznaczenie kraju/BC], zgodnie z wymaganiami zawartymi w specyfikacji UDFS. Uczestnicy mogą uzgodnić między sobą szczegółowe zasady dotyczące zawartości pól. Jednak w ramach systemu TARGET2-[oznaczenie kraju/BC] przestrzeganie tych zasad przez uczestników nie będzie badane.
- 4) Uczestnicy korzystający z dostępu przez Internet mogą dokonywać przez TARGET2 płatności pokrywających, tzn. płatności dokonanych przez banki korespondentów w celu rozliczenia (pokrycia) komunikatów poleceń przelewu, które zostają przekazane bankowi klienta za pomocą innych, bardziej bezpośrednich środków. Zawartych w tych płatnościach pokrywających szczegółów dotyczących klienta nie wyświetla się w ICM.

**3. Test na dwukrotne wprowadzenie**

- 1) Wszystkie zlecenia płatnicze przechodzą test na dwukrotne wprowadzenie, którego celem jest odrzucenie zleceń płatniczych, które zostały wprowadzone omyłkowo więcej niż jeden raz.

2) Sprawdzeniu podlegają następujące pola poszczególnych typów komunikatów:

Szczegóły	Część komunikatu	Pole
Wysyłający	Nagłówek podstawowy	Adres BIC
Typ komunikatu	Nagłówek aplikacji	Typ komunikatu
Odbiorca	Nagłówek aplikacji	Adres przeznaczenia
Numer referencyjny transakcji ( <i>Transaction Reference Number, TRN</i> )	Blok tekstowy	:20
Powiązane oznaczenie referencyjne	Blok tekstowy	:21
Data waluty	Blok tekstowy	:32
Kwota	Blok tekstowy	:32

3) Jeżeli wszystkie pola opisane w ust. 2 są dla nowo składanego zlecenia płatniczego identyczne jak w przypadku zlecenia płatniczego, które zostało już przyjęte, nowo składane zlecenie płatnicze podlega zwróceniu.

#### 4. Kody błędów

W przypadku odrzucenia zlecenia płatniczego udostępnia się przez ICM zawiadomienie o przerwaniu, wskazujące za pomocą kodów błędów przyczyny odrzucenia. Kody błędów są opisane w rozdziale 9.4.2 UDFS.

#### 5. Określenie terminu rozrachunku z wyprzedzeniem

- 1) Dla zleceń płatniczych wykorzystujących wskaźnik najwcześniejszego terminu obciążenia używa się słowa kodowego »/FROTIME/«.
- 2) Dla zleceń płatniczych wykorzystujących wskaźnik najpóźniejszego terminu obciążenia dostępne są dwie możliwości:
  - a) słowo kodowe »/REJTIME/«: jeżeli rozrachunek transakcji nie może nastąpić przed wskazanym terminem obciążenia, zlecenie płatnicze podlega zwróceniu;
  - b) słowo kodowe »/TILTIME/«: jeżeli rozrachunek zlecenia płatniczego nie może nastąpić przed wskazanym terminem obciążenia, zlecenie płatnicze nie podlega zwróceniu, ale zostaje umieszczone w odpowiedniej kolejce.

W obydwu przypadkach, jeżeli zlecenie płatnicze zawierające wskaźnik najpóźniejszego terminu obciążenia nie zostanie wykonane 15 minut przed wskazanym terminem, za pośrednictwem ICM automatycznie udostępnia się zawiadomienie.

- 3) W przypadku posłużenia się słowem kodowym »/CLSTIME/« płatność traktuje się tak samo jak zlecenie płatnicze, o którym mowa w ust. 2 lit. b).

#### 6. Rozrachunek zleceń płatniczych we wstępnej próbie przetwarzania

- 1) W celu umożliwienia szybkiego i oszczędzającego płynność rozrachunku brutto zleceń płatniczych zlecenia płatnicze wprowadzone do wstępnej próby przetwarzania poddaje się testowi na możliwość kompensowania lub, jeżeli jest to właściwe, rozszerzonemu testowi na możliwość kompensowania (zdefiniowanym w ust. 2 i 3).
- 2) Test na możliwość kompensowania służy sprawdzeniu, czy zlecenia płatnicze odbiorcy płatności znajdujące się na czele kolejki płatności oczekujących oznaczonych jako bardzo pilne, lub – jeżeli takich brak – jako pilne, mogą być przedmiotem kompensowania ze zleceniem płatniczym płatnika (dalej »płatności podlegające kompensowaniu«). Jeżeli płatność podlegająca kompensowaniu nie zapewnia wystarczających środków na pokrycie odpowiedniego zlecenia płatniczego płatnika we wstępnej próbie przetwarzania, ustala się, czy na rachunku w PM płatnika znajduje się wystarczająca dostępna płynność.

- 3) Jeżeli wynik testu na możliwość kompensowania jest negatywny, [nazwa BC] może zastosować rozszerzony test na możliwość kompensowania. Rozszerzony test na możliwość kompensowania służy sprawdzeniu, czy w którejkolwiek z kolejek płatności oczekujących należących do odbiorcy płatności znajdują się płatności podlegające kompensowaniu, niezależnie od chwili ich umieszczenia w danej kolejce. Jeżeli jednak w kolejce płatności oczekujących należących do odbiorcy płatności znajdują się zlecenia płatnicze oznaczone wyższym priorytetem zaadresowane do innych uczestników TARGET2, od zasady FIFO można odstąpić, wyłącznie gdy rozliczenie zlecenia płatniczego podlegającego kompensowaniu prowadziło do zwiększenia płynności odbiorcy płatności.

#### 7. Rozrachunek zleceń płatniczych w ramach kolejki zleceń oczekujących

- 1) Zlecenia płatnicze umieszczone w kolejkach zleceń oczekujących są traktowane w zależności od priorytetu, za pomocą którego dane zlecenie płatnicze zostało oznaczone przez uczestnika składającego instrukcję.
- 2) Zlecenia płatnicze znajdujące się w kolejkach płatności oczekujących oznaczonych jako bardzo pilne i pilne podlegają rozrachunkowi przy wykorzystaniu testów na możliwość kompensowania, o których mowa w punkcie 6, poczynając od zlecenia płatniczego znajdującego się na czele kolejki, w przypadku gdy prowadzi to do wzrostu płynności lub w przypadku gdy następuje ingerencja w ramach kolejki (zmiana pozycji w kolejce, terminu rozrachunku lub priorytetu, lub odwołanie zlecenia płatniczego).
- 3) Zlecenia płatnicze oczekujące w kolejce płatności oznaczonych jako zwykle podlegają rozrachunkowi w sposób ciągły, włącznie z wszystkimi zleceniami płatniczymi oznaczonymi jako bardzo pilne i pilne, które nie zostały jeszcze poddane rozrachunkowi. Stosuje się różne mechanizmy optymalizacji (algorytmy). Jeżeli zastosowanie algorytmu okaże się skuteczne, objęte nim zlecenia płatnicze podlegają rozrachunkowi; jeżeli algorytm okaże się nieskuteczny, objęte nim zlecenia płatnicze pozostają w kolejce. Stosuje się trzy algorytmy (1 do 3) w celu kompensowania przepływów płatności. Użycie algorytmu 4 umożliwia wykorzystanie procedury rozrachunkowej 5 (określonej w rozdziale 2.8.1 UDFS) dla rozrachunku instrukcji płatniczych systemów zewnętrznych. W celu optymalizacji rozrachunku na subkontach uczestników transakcji systemów zewnętrznych oznaczonych jako bardzo pilne stosuje się specjalny algorytm (algorytm 5).
- a) W ramach algorytmu 1 («wszystko albo nic»), [nazwa BC], zarówno w odniesieniu do każdego stosunku, dla którego ustalono limit dwustronny, jak i łącznej sumy stosunków, dla których ustalono limit wielostronny:
- (i) oblicza zbiorczą pozycję płynności dla rachunku w PM każdego uczestnika TARGET2, określając, czy suma wszystkich wychodzących i przychodzących zleceń płatniczych oczekujących w kolejce jest ujemna czy dodatnia, a jeżeli jest ona ujemna, sprawdza, czy przekracza ona dostępną płynność tego uczestnika (zbiorcza pozycja płynności stanowić będzie «całkowitą pozycję płynności»); oraz
  - (ii) sprawdza, czy są przestrzegane limity oraz blokady ustalone przez każdego z uczestników TARGET2 w odniesieniu do danego rachunku w PM.

Jeżeli rezultat powyższych obliczeń oraz sprawdzeń jest pozytywny dla każdego właściwego rachunku w PM, [nazwa BC] oraz pozostałe biorące udział BC dokonują jednoczesnego rozrachunku wszystkich płatności na rachunkach w PM uczestników TARGET2 biorących udział w rozrachunku.

- b) W ramach algorytmu 2 («częściowy»), [nazwa BC]:

- (i) oblicza i sprawdza pozycje płynności, limity i blokady dla każdego właściwego rachunku w PM w taki sam sposób jak w przypadku algorytmu 1; oraz
- (ii) jeżeli całkowita pozycja płynności na jednym lub kilku właściwych rachunkach w PM jest ujemna, usuwa pojedyncze zlecenia płatnicze do chwili, gdy całkowita pozycja płynności każdego z właściwych rachunków w PM stanie się dodatnia.

Następnie, jeżeli istnieją wystarczające środki, [nazwa BC] i pozostałe biorące udział BC dokonują jednoczesnego rozrachunku wszystkich pozostałych płatności (z wyjątkiem usuniętych zleceń płatniczych) na rachunkach w PM właściwych uczestników TARGET2.

Usuwanie zleceń płatniczych [nazwa BC] rozpoczyna od rachunku w PM uczestnika TARGET2 z najwyższą ujemną całkowitą pozycją płynności oraz od zlecenia płatniczego znajdującego się na końcu kolejki zleceń oczekujących oznaczonych najniższym priorytetem. Proces selekcji jest ograniczony do krótkiego czasu, określonego według uznania [nazwa BC].

- c) W ramach algorytmu 3 («wielokrotny»), [nazwa BC]:

- (i) porównuje pary rachunków w PM uczestników TARGET2 w celu ustalenia, czy zlecenia płatnicze oczekujące w kolejce mogą zostać poddane rozrachunkowi w ramach dostępnej płynności danej pary rachunków w PM uczestników TARGET2 przy uwzględnieniu ustalonych przez nich limitów (rozpoczynając od pary rachunków w PM z najniższą różnicą między zleceniami płatniczymi adresowanymi do siebie wzajemnie przez obydwie strony), a biorący(-e) udział BC dokonuje(-a) jednoczesnego zaksięgowania tych płatności na rachunkach w PM pary uczestników TARGET2; oraz



(ii) jeżeli w odniesieniu do pary rachunków w PM, o których mowa w podpunkcie (i) dostępna płynność jest niewystarczająca dla pokrycia pozycji dwustronnej, usuwa poszczególne zlecenia płatnicze do chwili, gdy dostępna płynność jest wystarczająca. W takim przypadku biorący(-e) udział BC dokonuje(-ą) jednoczesnego rozrachunku pozostałych płatności – z wyjątkiem tych usuniętych – na rachunkach w PM właściwych dwóch uczestników TARGET2.

Po dokonaniu sprawdzeń, o których mowa w podpunktach od (i) do (ii) [nazwa BC] weryfikuje wielostronne pozycje rozrachunkowe (pomiędzy rachunkiem w PM uczestnika a rachunkami w PM innych uczestników TARGET2, w odniesieniu do których ustalono limit wielostronny). W tym celu odpowiednio stosuje się procedurę, o której mowa w podpunktach od (i) do (ii).

- d) W ramach algorytmu 4 («częściowy plus rozrachunek Systemów Zewnętrznych») [nazwa BC] postępuje według takiej samej procedury jak w algorytmie 2, nie usuwa jednak zleceń płatniczych dotyczących rozrachunku systemu zewnętrznego (który następuje na zasadzie równoczesnego rozrachunku wielostronnego).
- e) W ramach algorytmu 5 («rozrachunek systemów zewnętrznych poprzez subkonta») [nazwa BC] postępuje według procedury algorytmu 1, z tą różnicą, że [nazwa BC] rozpoczyna algorytm 5 przez interfejs systemu zewnętrznego (*Ancillary System Interface, ASI*) i sprawdza jedynie, czy na subkontach uczestników dostępne są wystarczające środki. Ponadto nie uwzględnia się limitów i blokad. Algorytm 5 stosuje się również podczas rozliczeń nocnych.
- 4) Zlecenia płatnicze wprowadzone do wstępnej próby przetwarzania po uruchomieniu któregośkolwiek z algorytmów 1 do 4 mogą mimo wszystko podlegać rozrachunkowi natychmiast we wstępnej próbie przetwarzania, jeżeli pozycje i limity właściwych rachunków w PM uczestników TARGET2 umożliwiają zarówno rozrachunek tych zleceń płatniczych, jak i rozrachunek zleceń płatniczych w ramach bieżącej procedury optymalizacji. Nie jest jednak możliwe równoczesne stosowanie dwóch algorytmów.
- 5) W czasie przetwarzania dziennego algorytmy stosowane są według ustalonej kolejności. O ile nie jest w toku równoczesny rozrachunek wielostronny systemu zewnętrznego, kolejność ta jest następująca:
- a) algorytm 1;
  - b) jeżeli wynik algorytmu 1 jest negatywny – algorytm 2;
  - c) jeżeli wynik algorytmu 2 jest negatywny – algorytm 3 lub jeżeli wynik algorytmu 2 jest pozytywny – powtarza się algorytm 1.

Jeżeli równoczesny rozrachunek wielostronny («procedura 5») systemu zewnętrznego jest w toku, stosuje się algorytm 4.

- 6) Algorytmy stosuje się w sposób elastyczny dzięki określonemu z góry odstępowi czasowemu między uruchomieniami poszczególnych algorytmów w celu zapewnienia minimalnej przerwy między działaniem dwóch algorytmów. Nastęstwo czasowe podlega automatycznej kontroli. Możliwa jest również interwencja ręczna.
- 7) Po objęciu zlecenia płatniczego działaniem algorytmu nie jest możliwa zmiana jego pozycji w kolejce ani jego odwołanie. Wnioski o zmianę pozycji w kolejce lub odwołanie zlecenia płatniczego zostają umieszczone w kolejce do czasu zakończenia działania algorytmu. Jeżeli dane zlecenie płatnicze zostanie poddane rozrachunkowi w czasie działania algorytmu, wniosek o zmianę pozycji w kolejce lub odwołanie zlecenia podlega odrzuceniu. Jeżeli rozrachunek zlecenia płatniczego nie został dokonany, wnioski uczestnika uwzględnia się niezwłocznie.

## 8. Wykorzystywanie ICM

- 1) Moduł ICM może być wykorzystywany do wprowadzania zleceń płatniczych.
- 2) Moduł ICM może być wykorzystywany do pozyskiwania informacji i zarządzania płynnością.
- 3) Z wyjątkiem przechowywanych zleceń płatniczych oraz informacji dotyczących danych statycznych, w ICM dostępne są tylko dane dotyczące bieżącego dnia operacyjnego. Treść ekranów dostępna jest wyłącznie w języku angielskim.
- 4) Informacje udostępniane są w trybie »na żądanie«, co oznacza, że każdy uczestnik musi zwrócić się o udostępnienie mu informacji. Uczestnicy regularnie sprawdzają w ciągu dnia operacyjnego, czy w ICM nie pojawiły się ważne komunikaty.
- 5) Uczestnicy korzystający z dostępu przez Internet mają dostęp tylko do trybu użytkownika-aplikacja (*user-to-application mode, U2 A*). Tryb U2 A umożliwia bezpośrednią komunikację pomiędzy uczestnikiem a ICM. Informacje wyświetlane są w przeglądarce działającej na PC. Dalsze szczegóły zawarte są w Podręczniku użytkownika ICM.

- 6) Każdy użytkownik dysponuje przynajmniej jednym stanowiskiem z dostępem do Internetu w celu uzyskania dostępu do ICM w trybie U2 A.
- 7) Prawa dostępu do ICM przyznaje się za pomocą certyfikatów, z których korzystanie opisano w pełniejszy sposób w ust. 10–13.
- 8) Uczestnicy mogą również używać ICM do przekazywania płynności:
  - a) [wstawić, jeżeli ma zastosowanie] ze swojego rachunku w PM na swój rachunek poza PM;
  - b) między rachunkiem w PM a subkontami uczestnika; oraz
  - c) z rachunku w PM na rachunek lustrzany zarządzany przez system zewnętrzny.

#### 9. Specyfikacja UDFS oraz publikacje »ICM User Handbook« i »User Manual: Internet Access for the Public Key Certification Service«

Dalsze informacje szczegółowe oraz przykłady objaśniające powyższe zasady zawarte są w specyfikacji UDFS oraz w publikacji »ICM User Handbook« (Podręcznik użytkownika ICM), okresowo aktualizowanych i publikowanych w języku angielskim na stronach internetowych [nazwa BC] oraz systemu TARGET2, a także w publikacji »User Manual: Internet Access for the Public Key Certification Service« (Podręcznik użytkownika dotyczący dostępu przez Internet do usług certyfikacji klucza publicznego).

#### 10. Wydawanie, zawieszanie, reaktywacja, cofnięcie i odnawianie certyfikatów

- 1) Uczestnicy zwracają się do [nazwa BC] o wydanie certyfikatów w celu umożliwienia im dostępu do TARGET2-[oznaczenie BC/kraju] z wykorzystaniem dostępu przez Internet.
- 2) Uczestnicy zwracają się do [nazwa BC] o zawieszenie i reaktywację certyfikatów, jak również o cofnięcie i odnowienie certyfikatów, w przypadku gdy posiadacz certyfikatu nie zamierza już mieć dostępu do TARGET2 lub jeżeli uczestnik zaprzestaje swojej działalności w TARGET2-[oznaczenie BC/kraju] (np. w wyniku połączenia lub przejęcia).
- 3) Uczestnik dochowuje należytej ostrożności i podejmuje wszelkie środki organizacyjne w celu zapewnienia, aby certyfikaty były wykorzystywane wyłącznie w sposób zgodny ze zharmonizowanymi warunkami.
- 4) Uczestnicy niezwłocznie powiadamiają [nazwa BC] o jakichkolwiek zmianach w zakresie treści jakichkolwiek informacji zawartych w formularzach złożonych do [nazwa BC] w związku z wydaniem certyfikatów.
- 5) Uczestnik może posiadać nie więcej niż 5 aktywnych certyfikatów dla każdego rachunku w PM. Na żądanie, [nazwa BC] może również złożyć według swojego uznania o wydanie kolejnych certyfikatów wnioski przez organy certyfikacyjne.

#### 11. Postępowanie uczestnika z certyfikatami

- 1) Uczestnik zapewnia bezpieczne przechowywanie certyfikatów i podejmuje skuteczne środki organizacyjne i techniczne w celu uniknięcia uszkodzenia osób trzecich oraz zapewnienia używania certyfikatów wyłącznie przez posiadacza certyfikatu, któremu został on wydany.
- 2) Uczestnik dostarcza niezwłocznie wszelkich informacji żądanych przez [nazwa BC] i gwarantuje rzetelność tych informacji. Uczestnik ponosi również ciągłą i pełną odpowiedzialność za stałą dokładność informacji dostarczanych [nazwa BC] w związku z wydawaniem certyfikatów.
- 3) Uczestnik ponosi pełną odpowiedzialność za zapewnienie, aby wszyscy wskazani przez niego posiadacze certyfikatów przechowywali przydzielone im certyfikaty oddzielnie od tajnych kodów PIN i PUK.
- 4) Uczestnik ponosi pełną odpowiedzialność za zapewnienie, aby żaden ze wskazanych przez niego posiadaczy certyfikatów nie korzystał z certyfikatów w innych celach lub funkcjach niż te, dla których certyfikaty zostały wydane.
- 5) Uczestnik informuje niezwłocznie [nazwa BC] o jakichkolwiek wnioskach o zawieszenie, reaktywację, cofnięcie lub odnowienie certyfikatów oraz o powodach tych czynności.
- 6) Uczestnik niezwłocznie zwraca się do [nazwa BC] o zawieszenie jakichkolwiek certyfikatów lub zawartych w nich kluczy, które dotknięte zostały defektem albo nie są już w posiadaniu wskazanych przez niego posiadaczy certyfikatów.
- 7) Uczestnik informuje niezwłocznie [nazwa BC] o jakimkolwiek przypadku utraty lub kradzieży certyfikatów.

## 12. Wymogi dotyczące bezpieczeństwa

- 1) System komputerowy używany przez uczestnika do uzyskiwania dostępu do TARGET2 z wykorzystaniem dostępu przez Internet powinien znajdować się w lokalu będącym własnością uczestnika, lub którego najemcą jest uczestnik. Dostęp do TARGET2-[oznaczenie BC/kraju] dozwolony jest jedynie z takiego lokalu, przy czym, dla uniknięcia wątpliwości, nie zezwala się na dostęp zdalny.
- 2) Uczestnik korzysta z wszelkiego oprogramowania na systemach komputerowych zainstalowanych i posiadających indywidualne ustawienia zgodne z aktualnymi międzynarodowymi standardami bezpieczeństwa IT, które powinny co najmniej zawierać wymogi określone w pkt 12 ust. 3 i pkt 13 ust. 4. Uczestnik przyjmuje odpowiednie środki, w tym w szczególności zapewniające ochronę przed wirusami i złośliwym oprogramowaniem, zapobiegające wykradaniu haseł, jak również procedury podnoszenia poziomu bezpieczeństwa oraz wprowadzania poprawek do oprogramowania. Uczestnik regularnie aktualizuje wszelkie takie środki i procedury.
- 3) Uczestnik zakłada zaszyfrowane połączenie komunikacyjne z TARGET2-[oznaczenie BC/kraju] dla dostępu przez Internet.
- 4) Konta użytkowników na stacjach roboczych uczestnika nie mają uprawnień administratora. Uprawnienia przyznaje się zgodnie z zasadą »jak najmniejszych uprawnień«.
- 5) Uczestnicy zapewniają ciągłą ochronę systemów komputerowych używanych dla dostępu przez Internet do TARGET2-[oznaczenie BC/kraju] w następujący sposób:
  - a) Uczestnicy chronią systemy komputerowe i stacje robocze przed nieuprawnionym dostępem – fizycznym i sieciowym – używając przez cały czas zapory sieciowej (*firewall*) dla osłony systemów komputerowych i stacji roboczych przed danymi odbieranymi z Internetu, jak również stacji roboczych przed nieuprawnionym dostępem przez sieć wewnętrzną. Uczestnicy używają zapory sieciowej chroniącej przed danymi odbieranymi z internetu, jak również zapory sieciowej na stacjach roboczych umożliwiającej komunikowanie się na zewnątrz wyłącznie autoryzowanym programom.
  - b) Uczestnicy są uprawnieni do zainstalowania na stacjach roboczych jedynie oprogramowania niezbędnego do dostępu do TARGET2 oraz takiego, które jest dozwolone zgodnie ze stosowanymi przez uczestnika wewnętrznymi zasadami bezpieczeństwa.
  - c) Uczestnicy zapewniają w sposób ciągły, aby wszystkie elementy oprogramowania stosowane na stacjach roboczych były regularnie aktualizowane i uzupełniane poprawkami zgodnie z najnowszą wersją. Dotyczy to w szczególności systemu operacyjnego, przeglądarki internetowej oraz dodatków.
  - d) Uczestnicy w sposób ciągły ograniczają wychodzący przepływ danych ze stacji roboczych do stron mających największe znaczenie dla ich działalności, jak również do stron koniecznych dla przeprowadzania uprawnionych i uzasadnionych aktualizacji oprogramowania.
  - e) Uczestnicy zapewniają ochronę wszystkich krytycznych wewnętrznych przepływów danych do stacji roboczych i z tych stacji przed ujawnieniem i szkodliwymi zmianami, w szczególności w razie przesyłania plików przez sieć.
- 6) Uczestnicy zapewniają ciągłe przestrzeganie przez wskazanych przez nich posiadaczy certyfikatów zasad bezpiecznego korzystania z Internetu, w tym:
  - a) rezerwowanie określonych stacji roboczych do dostępu do stron o tym samym poziomie znaczenia i łączenie się z tymi stronami wyłącznie z tych stacji roboczych;
  - b) ponowne uruchamianie sesji przeglądarki zawsze przed i po uzyskaniu dostępu do TARGET2-[oznaczenie BC/kraju] przez Internet;
  - c) weryfikację certyfikatu SSL każdego serwera przy każdym logowaniu do TARGET2-[oznaczenie BC/kraju] przez Internet;
  - d) ostrożne traktowanie e-maili, które wydają się pochodzić od TARGET2-[oznaczenie BC/kraju] oraz niepodawanie hasła certyfikatu w przypadku otrzymania pytania o to hasło, ponieważ TARGET2-[oznaczenie BC/kraju] nigdy nie zwraca się o podanie hasła certyfikatu e-mailem lub w inny sposób.
- 7) Dla ograniczenia ryzyka dla swojego systemu uczestnik stale stosuje się do następujących zasad zarządzania:
  - a) ustalenie praktyki zarządzania użytkownikami zapewniającej zakładanie i utrzymywanie w systemie jedynie kont uprawnionych użytkowników, jak również utrzymywanie dokładnej i aktualnej listy uprawnionych użytkowników;

- b) porównywanie dziennego przepływu płatności w celu wykrycia niezgodności pomiędzy autoryzowanym a faktycznym przepływem płatności, zarówno wysyłanych, jak i otrzymanych;
- c) uniemożliwienie posiadaczowi certyfikatu przeglądania innych stron internetowych w tym samym czasie, w którym uzyskuje dostęp do TARGET2-[oznaczenie BC/kraju].

### 13. Dodatkowe wymogi dotyczące bezpieczeństwa

- 1) Uczestnik w sposób ciągły zapewnia, przez stosowanie odpowiednich środków organizacyjnych lub technicznych, aby nie dochodziło do nadużywania danych identyfikacyjnych użytkownika ujawnionych w celu kontroli uprawnień dostępu (procedura przeglądu uprawnień dostępu – *Access Right Review*), w szczególności, aby wiedzy o nich nie uzyskiwały osoby nieuprawnione.
  - 2) Uczestnik stosuje procedurę administracji użytkownikami w celu zapewnienia niezwłocznego i trwałego usunięcia danych identyfikacyjnych użytkownika w przypadku, gdy pracownik lub inny użytkownik systemu w lokalu uczestnika opuszcza instytucję uczestnika.
  - 3) Uczestnik stosuje procedurę administracji użytkownikami i niezwłocznie i trwale blokuje dane identyfikacyjne użytkownika, które zostały w jakikolwiek sposób zagrożone, w tym w przypadku utraty lub kradzieży certyfikatów, jak również wykradzenia hasła.
  - 4) Jeżeli uczestnik nie jest w stanie usunąć usterek w zakresie bezpieczeństwa lub błędów konfiguracji (np. wynikających z zainfekowania systemu złośliwym oprogramowaniem), po ich trzykrotnym wystąpieniu BC dostarczający SSP może trwale zablokować dane identyfikacyjne wszystkich użytkowników od danego uczestnika.
-

*Dodatek IIA***TARYFA OPŁAT I FAKTUROWANIE DLA DOSTĘPU PRZEZ INTERNET****Opłaty dla uczestników bezpośrednich**

1. Opłata miesięczna za przetwarzanie zleceń płatniczych w systemie TARGET2-[oznaczenie BC/kraju] wynosi dla uczestników bezpośrednich 70 EUR za rachunek w PM opłaty za dostęp przez Internet, 100 EUR opłaty za rachunek w PM oraz jednolitą opłatę za każdą transakcję (obciążenie rachunku) w wysokości 0,80 EUR.
2. Od uczestników bezpośrednich, którzy nie życzą sobie publikacji BIC ich rachunków w TARGET2 directory, pobierana będzie dodatkowa miesięczna opłata w wysokości 30 EUR od każdego rachunku.

**Fakturowanie**

3. W przypadku uczestników bezpośrednich stosuje się następujące zasady fakturowania. Uczestnik bezpośredni otrzymuje fakturę za poprzedni miesiąc określającą opłaty do zapłaty nie później niż piątego dnia operacyjnego kolejnego miesiąca. Zapłata następuje najpóźniej dziesiątego dnia operacyjnego tego miesiąca na rachunek wskazany przez [nazwa BC] i zostaje ona pobrana z rachunku w PM danego uczestnika.”
-