DECYZJE

DECYZJA EUROPEJSKIEGO BANKU CENTRALNEGO

z dnia 11 stycznia 2013 r.

ustanawiająca ramy infrastruktury klucza publicznego Europejskiego Systemu Banków Centralnych

(EBC/2013/1)

(2013/132/UE)

RADA PREZESÓW EUROPEJSKIEGO BANKU CENTRALNEGO,

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

uwzględniając Statut Europejskiego Systemu Banków Centralnych i Europejskiego Banku Centralnego (zwany dalej „Statutem ESBC"), w szczególności jego art. 12 ust. 1 w związku z art. 3 ust. 1, art. 5, art. 12 ust. 3 oraz art. 16–24,

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 12 ust. 1 Statutu ESBC Rada Prezesów uchwala wytyczne i podejmuje decyzje niezbędne do zapewnienia wykonania zadań powierzonych Europejskiemu Systemowi Banków Centralnych (ESBC) i Eurosystemowi na podstawie Traktatu i Statutu ESBC. Obejmuje to określanie sposobu organizacji działań dodatkowych, niezbędnych do wykonywania tych zadań, takich jak wydawanie i zarządzanie elektronicznymi certyfikatami służącymi do ochrony informacji przechowywanych i przetwarzanych w elektronicznych aplikacjach, systemach, platformach i usługach ESBC i Eurosystemu, oraz do przekazywania im danych i ich odbierania.

(2) Zgodnie z art. 12 ust. 3 Statutu ESBC Rada Prezesów ma również kompetencje do określania organizacji wewnętrznej Europejskiego Banku Centralnego (EBC) i jego organów decyzyjnych. Rada Prezesów jest zatem również władna zdecydować o korzystaniu przez EBC z certyfikatów elektronicznych wydawanych przez własną infrastrukturę klucza publicznego Eurosystemu.

(3) Zwiększa się liczba użytkowników korzystających z rosnącej liczby nieustannie zmieniających się elektronicznych aplikacji, systemów, platform i usług ESBC i Eurosystemu. Rada Prezesów stwierdziła zapotrzebowanie na zaawansowane usługi w zakresie bezpieczeństwie informacji, takie jak silne uwierzytelnianie, podpisy elektroniczne i szyfrowanie za pośrednictwem certyfikatów elektronicznych.

(4) Jedynie niektóre banki centralne ESBC posiadają własną infrastrukturę klucza publicznego, a wielu użytkowników z podmiotów trzecich współpracujących z bankami centralnymi ESBC ma utrudniony dostęp do organów certyfikacji zatwierdzonych przez ESBC zgodnie z zasadami akceptacji certyfikatów ESBC.

(5) Istnieje potrzeba, aby Eurosystem stworzył swoją własną infrastrukturę klucza publicznego, która będzie mogła wydawać wszystkie rodzaje certyfikatów elektronicznych, takie jak certyfikaty osobiste i certyfikaty techniczne dla użytkowników z ESBC i spoza ESBC i która będzie na tyle elastyczna, by dostosowywać się do zmian w elektronicznych aplikacjach, systemach, platformach i usługach ESBC i Eurosystemu. Wspomniana infrastruktura klucza publicznego (zwana dalej „PKI ESBC") powinna uzupełniać usługi świadczone przez inne organy certyfikacji zaakceptowane przez ESBC zgodnie z zasadami akceptacji certyfikatów ESBC lub przez organy certyfikacji zaakceptowane przez ESBC w odniesieniu do TARGET2 i TARGET2 Securities dla tych dwóch aplikacji.

(6) W dniu 29 września 2010 r. Rada Prezesów podjęła decyzję o rozpoczęciu projektu infrastruktury klucza publicznego ESBC w celu zbudowania i wdrożenia PKI ESBC oraz o przeznaczeniu na ten cel środków niezbędnych do jego pełnej realizacji. Rada Prezesów zdecydowała, że podmiotem odpowiedzialnym za stworzenie, hosting i obsługę PKI ESBC będzie Banco de España.

(7) PKI ESBC pośrednio wspiera wykonywanie zadań ESBC i Eurosystemu. Działanie PKI ESBC opera się na trzech poziomach zarządzania: na poziom 1 składa się Rada Prezesów i Zarząd, na poziom 2 – banki centralne Eurosystemu, na poziom 3 – dostarczający bank centralny.

(8) Na poziomie 1 Rada Prezesów jest odpowiedzialna za kierowanie i zarządzanie działaniami i świadczeniami niezbędnymi do opracowania i obsługi PKI ESBC, oraz ich kontrolowaniem. Radzie Prezesów przysługują także kompetencje decyzyjne w zakresie PKI ESBC oraz kompetencje do podejmowania decyzji o podziale zadań niezastrzeżonych wyraźnie do kompetencji poziomu 2 lub 3.

(9) Banki centralne Eurosystemu są odpowiedzialne za realizację zadań przypisanych poziomowi 2 w ramach ogólnych zasad określonych przez Radę Prezesów. Bankom centralnym Eurosystemu przysługują kompetencje w zakresie technicznych środków wdrożenia PKI ESBC.

(10) Wiodącą rolę w opracowaniu PKI ESBC ma Komitet ESBC ds. Informatyki. Komitet ESBC ds. Informatyki doradza, ocenia, kontroluje i zatwierdza świadczenia dostarczane w ramach projektu w kontekście kryteriów akceptacji zgodnie z zasadami akceptacji certyfikatów ESBC, zakresem i harmonogramem zatwierdzonym przez Radę Prezesów.

(11) Na poziomie 3 Banco de España został wyznaczony na dostarczający bank centralny wypełniający zadania przydzielone mu w ramach ogólnych zasad określonych przez Radę Prezesów. Dostarczający bank centralny wprowadził infrastrukturę techniczną oraz bezpieczne urządzenia i usługi niezbędne od opracowania i używania infrastruktury klucza publicznego zgodnie z: a) przepisami prawa krajowego stanowiącymi transpozycję dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych ([1]), w zakresie mającym do niego zastosowanie; b) przepisami prawa krajowego stanowiącymi transpozycję dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([2]), w zakresie mającym do niego zastosowanie; oraz c) rozporządzeniem (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ([3]).

(12) Jako że certyfikaty elektroniczne są niezbędnym elementem wykorzystywanym w aplikacjach elektronicznych, zarówno jako mechanizm uwierzytelniania przy składaniu podpisów elektronicznych, jak i dla celów szyfrowania opartego na kluczu publicznym, PKI ESBC będzie obejmować istniejące elektroniczne aplikacje, systemy, platformy i usługi ESBC i Eurosystemu oraz realizowane obecnie projekty ESBC, w celu uwzględnienia ich potrzeb.

(13) Krajowe banki centralne (KBC) spoza strefy euro mogą zdecydować się na korzystanie z certyfikatów i usług dostarczanych przez PKI ESBC,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Definicje

Dla celów niniejszej decyzji użyte w niej określenia oznaczają:

1) „certyfikat" lub „certyfikat elektroniczny" – wydany przez organ certyfikacji elektroniczny plik łączący klucz publiczny z tożsamością subskrybenta certyfikatu, używany do wszystkich lub niektórych z następujących celów: a) weryfikowania, czy klucz publiczny należy do subskrybenta certyfikatu; b) uwierzytelniania subskrybenta certyfikatu; c) sprawdzania podpisu subskrybenta certyfikatu; d) szyfrowania komunikatu adresowanego do subskrybenta certyfikatu; e) weryfikowania praw dostępu subskrybenta certyfikatu do elektronicznych aplikacji, systemów, platform i usług ESBC i Eurosystemu. Zawarte w niniejszej decyzji odniesienia do certyfikatu lub certyfikatu elektronicznego obejmują odniesienia do nośników danych, na których taki certyfikat lub certyfikat elektroniczny jest przechowywany;

2) „elektroniczne aplikacje, systemy, platformy i usługi ESBC i Eurosystemu" – elektroniczne aplikacje, systemy, platformy i usługi wykorzystywane przez Eurosystem lub ESBC do wykonywania zadań powierzonych im na mocy Traktatu i Statutu ESBC;

3) „infrastruktura klucza publicznego" – zbiór osób, polityk, procedur i systemów komputerowych niezbędnych do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego i prywatnego i certyfikatów elektronicznych;

4) „użytkownik" – subskrybenta certyfikatu, stronę ufającą lub obydwa te podmioty;

5) „uwierzytelnianie" – proces weryfikacji tożsamości podmiotu wnioskującego o certyfikat lub subskrybenta certyfikatu;

6) „bank centralny ESBC" – bank centralny Eurosystemu lub KBC spoza strefy euro;

7) „bank centralny Eurosystemu" – KBC państwa członkowskiego, którego walutą jest euro, w tym dostarczający bank centralny, lub EBC;

8) „dostarczający bank centralny" – KBC wyznaczony przez Radę Prezesów do opracowania PKI ESBC oraz do świadczenia usług PKI ESBC w imieniu i na rzecz banków centralnych Eurosystemu;

9) „KBC spoza strefy euro" – KBC państwa członkowskiego, którego walutą nie jest euro;

10) „organ certyfikacji PKI ESBC" – podmiot, który jest zaufanym podmiotem użytkowników w zakresie wydawania, unieważniania i odnawiania certyfikatów lub zarządzaniami nimi w imieniu banków centralnych ESBC lub banków centralnych Eurosystemu zgodnie z zasadami akceptacji certyfikatów ESBC;

11) „organ walidacji PKI ESBC" – podmiot, który jest zaufanym podmiotem użytkowników w zakresie dostarczania informacji o ważności certyfikatów wydawanych przez organ certyfikacji PKI ESBC;

12) „subskrybent certyfikatu" – osobę, która jest podmiotem certyfikatu elektronicznego i której wydano certyfikat elektroniczny, lub menedżera elementu technicznego, który zaakceptował certyfikat elektroniczny wydany przez organ certyfikacji PKI ESBC dla elementu technicznego, lub obydwa te podmioty;

13) „zasady akceptacji certyfikatów ESBC" – kryteria ustanowione przez Komitet ESBC ds. Informatyki dla potrzeb identyfikacji organów certyfikacji, zarówno wewnętrznych,

([1]) Dz.U. L 13 z 19.1.2000, s. 12.
([2]) Dz.U. L 281 z 23.11.1995, s. 31.
([3]) Dz.U. L 8 z 12.1.2001, s. 1.

jak i spoza ESBC, które są zaufanymi organami w odniesieniu do elektronicznych aplikacji, systemów, platform i usług ESBC i Eurosystemu;

14) „organ rejestracji" – organ, który jest zaufanym organem użytkowników w zakresie weryfikowania tożsamości podmiotu wnioskującego o certyfikat przed wydaniem certyfikatu przez organ certyfikacji PKI ESBC;

15) „strona ufająca" – osobę lub podmiot niebędący subskrybentem certyfikatu, akceptujący certyfikat i ufający mu;

16) „polityka audytu" – politykę audytu ESBC ustanowioną przez Radę Prezesów dnia 7 października 1998 r. i opublikowaną na stronie internetowej EBC ([1]);

17) „podmiot wnioskujący o certyfikat" – osobę, która wnioskuje o wydanie certyfikatu dla siebie lub dla elementu technicznego;

18) „element techniczny" – oprogramowanie lub sprzęt, który może być zidentyfikowany przy użyciu certyfikatu elektronicznego.

Artykuł 2

Zakres

1. Niniejsza decyzja ustanawia ramy PKI ESBC. PKI ESBC jest własną infrastrukturą klucza publicznego Eurosystemu stworzoną przez dostarczający bank centralny w imieniu i na rzecz banków centralnych Eurosystemu, która wydaje, unieważnia i odnawia certyfikaty oraz zarządza nimi zgodnie z zasadami akceptacji certyfikatów ESBC.

2. Jako że usługi PKI ESBC mogą mieć wpływ na strony ufające, niniejsza decyzja określa także warunki, na jakich takie strony mogą ufać certyfikatom wydawanym przez PKI ESBC.

Artykuł 3

Zakres i cele PKI ESBC

1. Dostęp do elektronicznych aplikacji, systemów, platform i usług ESBC i Eurosystemu o poziomie znaczenia średnim lub wyższym niż średni i korzystanie z nich jest możliwe tylko dla użytkowników, którzy zostali uwierzytelnieni przez certyfikat elektroniczny wydany i obsługiwany przez organ certyfikacji zaakceptowany przez ESBC zgodnie z zasadami akceptacji certyfikatów ESBC, w tym przez organ certyfikacji PKI ESBC, lub przez organy certyfikacji zaakceptowane przez ESBC w odniesieniu do TARGET2 i TARGET2 Securities dla tych dwóch aplikacji.

2. Organ certyfikacji PKI ESBC wydaje certyfikaty elektroniczne i świadczy inne usługi certyfikacji elektronicznej na rzecz subskrybentów certyfikatu banków centralnych ESBC i podmiotów trzecich z nimi współpracujących w celu umożliwienia im bezpiecznego dostępu i wykorzystania elektronicznych aplikacji, systemów, platform i usług ESBC i Eurosystemu.

3. PKI ESBC świadczy następujące usługi certyfikacyjne:

a) wydawanie, odnawianie i unieważnianie certyfikatów oraz potwierdzanie ważności certyfikatu w odniesieniu do różnych typów certyfikatów;

b) wydawanie certyfikatów do uwierzytelniania, podpisów elektronicznych i szyfrowania, w odniesieniu do użytkowników z ESBC i spoza ESBC, oraz certyfikatów technicznych;

c) odtwarzanie klucza prywatnego w celu odtworzenia zaszyfrowanych informacji opartych na kluczu publicznym w przypadku utraty certyfikatu;

d) w razie potrzeby – dostarczanie tokenów kryptograficznych subskrybentom certyfikatu i zarządzanie tymi tokenami;

e) przekazywanie informacji dotyczących procedur zarządzania certyfikatami PKI ESBC oraz wsparcie techniczne dla menedżerów projektu ESBC w zakresie zintegrowania certyfikatów PKI ESBC z ich aplikacjami.

W przyszłości możliwe jest dodanie innych usług wymaganych przez elektroniczne aplikacje, systemy, platformy i usługi ESBC i Eurosystemu.

Artykuł 4

Ramy PKI ESBC

1. Z zastrzeżeniem postanowień niniejszej decyzji obowiązki i funkcje dostarczającego banku centralnego i innych banków centralnych Eurosystemu w odniesieniu do wdrożenia, obsługi i wykorzystania PKI ESBC określa umowa pomiędzy poziomami 2 i 3, której uszczegółowieniem są polityki certyfikacji PKI ESBC oraz kodeks postępowania certyfikacyjnego PKI ESBC.

2. Umowa pomiędzy poziomami 2 i 3, która obejmuje umowę o gwarantowanym poziomie usług, zawiera porozumienia wynegocjowane pomiędzy dostarczającym bankiem centralnym a bankami centralnymi Eurosystemu w odniesieniu do obowiązków i funkcji dostarczającego banku centralnego i banków centralnych Eurosystemu. Umowę pomiędzy poziomami 2 i 3 przedstawia się do zatwierdzenia Radzie Prezesów, a następnie przekazuje do podpisania przez dostarczający bank centralny i banki centralne Eurosystemu.

3. Umowa o gwarantowanym poziomie usług jest zarówno umową określającą poziom usług świadczonych przez dostarczający bank centralny na rzecz Eurosystemu, jak i umową określającą poziom usług świadczonych przez Eurosystem na rzecz KBC spoza strefy euro i podmiotów trzecich, w odniesieniu do PKI ESBC.

4. Kodeks postępowania certyfikacyjnego PKI ESBC jest zbiorem zasad dotyczących okresu stosowania certyfikatów elektronicznych od początkowego wniosku do zakończenia lub unieważnienia subskrypcji, jak również stosunków pomiędzy podmiotem wnioskującym o certyfikat lub subskrybentem certyfikatu, organem certyfikacji PKI ESBC oraz stronami ufającymi. Kodeks postępowania certyfikacyjnego PKI ESBC dotyczy zarówno certyfikatów elektronicznych objętych zakresem dyrektywy 1999/93/WE, jak i certyfikatów elektronicznych nieobjętych zakresem tej dyrektywy. Kodeks postępowania certyfikacyjnego PKI ESBC określa również role i obowiązki wszystkich stron i ustanawia procedury dotyczące wydawania certyfikatów i zarządzania nimi. Kodeks postępowania certyfikacyjnego PKI ESBC stanowi załącznik do umowy pomiędzy poziomami 2 i 3.

([1]) www.ecb.europa.eu.

5. Polityki certyfikacji PKI ESBC są zbiorami zasad mających zastosowanie do każdego z typów wydawanych certyfikatów. Każdy z tych zbiorów określa szczegóły wdrożenia dotyczące kodeksu postępowania certyfikacyjnego PKI ESBC dla poszczególnych typów wydawanych certyfikatów. Polityki certyfikacji PKI ESBC stanowią załącznik do umowy pomiędzy poziomami 2 i 3.

6. Polityki certyfikacji PKI ESBC i kodeks postępowania certyfikacyjnego PKI ESBC publikuje się na stronie internetowej PKI ESBC ([1]).

7. Informacje dotyczące organu certyfikacji PKI ESBC, w tym jego tożsamości oraz elementów technicznych, są zawarte w załączniku do niniejszej decyzji.

Artykuł 5

Obowiązki i role dostarczającego banku centralnego

1. Dostarczający bank centralny jest odpowiedzialny za obsługę i utrzymanie PKI ESBC na rzecz banków centralnych Eurosystemu, w tym hosting, obsługę i zarządzanie wykonywane zgodnie z umową pomiędzy poziomami 2 i 3. W szczególności dostarczający bank centralny dostarcza certyfikaty i świadczy usługi PKI ESBC w sposób zgodny z wymaganiami biznesowymi i specyfikacjami technicznymi, takimi jak zasady akceptacji certyfikatów ESBC oraz wymogi i specyfikacje określone w umowie pomiędzy poziomami 2 i 3.

2. Dostarczający bank centralny dostarcza wszelką infrastrukturę organizacyjną niezbędną do tworzenia i wydawania certyfikatów oraz zarządzania nimi oraz zapewnia utrzymywanie tej infrastruktury. W tym celu, w porozumieniu z Komitetem ESBC ds. Informatyki, dostarczający bank centralny może przyjmować regulaminy dotyczące swojej organizacji i administracji wewnętrznej.

3. Dostarczający bank centralny pełni funkcje organu certyfikacji PKI ESBC i organu walidacji PKI ESBC.

4. Zasady ponoszenia odpowiedzialności przez dostarczający bank centralny określa umowa pomiędzy poziomami 2 i 3.

Artykuł 6

Obowiązki i role banków centralnych Eurosystemu

1. Każdy z banków centralnych Eurosystemu jest odpowiedzialny za identyfikację swoich subskrybentów certyfikatów. Każdy z banków centralnych Eurosystemu tworzy stanowisko specjalisty ds. rejestracji odpowiedzialnego za realizację tego zadania, który dysponuje uprawnieniami do rejestrowania użytkowników będących osobami trzecimi.

2. Każdy z banków centralnych Eurosystemu jest stroną ufającą w odniesieniu do certyfikatów szyfrowania i podpisów elektronicznych wydanych przez PKI ESBC na rzecz innych banków centralnych Eurosystemu lub subskrybentów certyfikatów użytkowników będących osobami trzecimi.

3. Każdy z banków centralnych Eurosystemu korzystających z usług PKI ESBC jest organem rejestracji dla swoich podmiotów wnioskujących o certyfikat i zapewnia akceptację i stosowanie przez te podmioty warunków użytkownika zawartych we wniosku o udostępnienie usług organu certyfikacji PKI ESBC.

([1]) http://pki.escb.eu.

Artykuł 7

Stosunki pomiędzy bankami centralnymi Eurosystemu, osobami trzecimi i subskrybentami certyfikatów

Każdy z banków centralnych Eurosystemu zawiera porozumienia dotyczące bezpiecznego dostępu osób trzecich i stosowania elektronicznych aplikacji, systemów, platform i usług ESBC i Eurosystemu za pośrednictwem certyfikatów PKI ESBC. Porozumienia te regulują wyłącznie stosunki pomiędzy danym bankiem centralnym Eurosystemu a osobami trzecimi korzystającymi z certyfikatów PKI ESBC. Osoby trzecie są zobowiązane do przestrzegania polityk certyfikacji PKI ESBC, kodeksu postępowania certyfikacyjnego PKI ESBC oraz warunków użytkownika zawartych we wniosku o udostępnienie usług organu certyfikacji PKI ESBC.

Artykuł 8

Stosunki ze stronami ufającymi

Certyfikat elektroniczny wydany na podstawie niniejszej decyzji może być zaufanym certyfikatem, jeżeli strona ufająca:

a) zweryfikuje ważność, zawieszenie lub unieważnienie certyfikatu korzystając z aktualnych informacji o statusie unieważnienia certyfikatu;

b) uwzględni wszelkie ograniczenia używania określone w certyfikacie; oraz

c) zaakceptuje kodeks postępowania certyfikacyjnego PKI ESBC oraz mające zastosowanie polityki certyfikacji PKI ESBC.

Artykuł 9

Prawa do PKI ESBC

1. PKI ESBC stanowi w pełni własność banków centralnych Eurosystemu.

2. W związku z powyższym dostarczający bank centralny udzieli bankom centralnym Eurosystemu, w zakresie możliwym zgodnie z mającymi zastosowanie przepisami prawa, wszelkich licencji obejmujących prawa własności intelektualnej, niezbędnych do umożliwienia korzystania przez banki centralne Eurosystemu z PKI ESBC i jego elementów oraz pełnego zakresu usług PKI ESBC, a także świadczenia usług PKI ESBC na rzecz osób trzecich zgodnie z kodeksem postępowania certyfikacyjnego PKI ESBC i politykami certyfikacji PKI ESBC. Dostarczający bank centralny pokryje bankom centralnym Eurosystemu wszelkie roszczenia podnoszone przez osoby trzecie z tytułu naruszenia wspomnianych praw własności intelektualnej.

3. Szczegółowe ustalenia dotyczące praw banków centralnych Eurosystemu do PKI ESBC zostaną uzgodnione pomiędzy poziomem 2 a poziomem 3 w umowie pomiędzy poziomami 2 i 3.

Artykuł 10

Odpowiedzialność banków centralnych Eurosystemu względem użytkowników

1. Bank centralny Eurosystemu, o ile nie wykaże braku niedbalstwa, ponosi odpowiedzialność w ramach swoich funkcji

i obowiązków w PKI ESBC za szkody poniesione przez użytkownika, który w uzasadniony sposób zaufał certyfikatowi kwalifikowanemu w rozumieniu dyrektywy 1999/93/WE, w odniesieniu do:

a) dokładności – w momencie wydania certyfikatu – wszelkich informacji zawartych w kwalifikowanym certyfikacie, oraz kwestii zawarcia w certyfikacie wszystkich szczegółów, jakie powinien zawierać certyfikat kwalifikowany zgodnie z dyrektywą 1999/93/WE;

b) zagwarantowania, że w momencie wydania certyfikatu kwalifikowanego subskrybent certyfikatu w nim wskazany posiadał dane utworzenia podpisu odpowiadające danym weryfikacji podpisu podanym lub wskazanym w certyfikacie;

c) zagwarantowania, że urządzenie do składania podpisu i urządzenie do weryfikacji podpisu funkcjonują wspólnie w sposób komplementarny, w przypadku gdy PKI ESBC generuje obydwa te składniki;

d) nieudanego unieważnienia kwalifikowanego certyfikatu.

2. Poza przypadkami w sposób wyraźny wskazanymi w niniejszej decyzji oraz kodeksie postępowania certyfikacyjnego PKI ESBC banki centralne Eurosystemu nie podejmują wobec użytkowników zobowiązań, nie udzielają im gwarancji i nie ponoszą wobec nich odpowiedzialności.

Artykuł 11

Udział KBC spoza strefy euro w PKI ESBC

1. KBC spoza strefy euro może być organem rejestracji dla swoich użytkowników wewnętrznych oraz użytkowników będących osobami trzecimi, jak również może stworzyć stanowisko specjalisty ds. rejestracji odpowiedzialnego za realizację tego zadania.

2. Po uzyskaniu zgody Rady Prezesów KBC spoza strefy euro może także zdecydować się na korzystanie z usług PKI ESBC na tych samych warunkach, jakie mają zastosowanie do banków centralnych Eurosystemu. W tym celu KBC spoza strefy euro składa Radzie Prezesów deklarację, w której potwierdza, że będzie wypełniał obowiązki określone w niniejszej decyzji oraz umowie pomiędzy poziomami 2 i 3. KBC spoza strefy euro nie staje się współwłaścicielem PKI ESBC i nie jest zobowiązany do wnoszenia wkładu do ram finansowych PKI ESBC.

Artykuł 12

Ochrona danych

Banki centralne Eurosystemu są zobowiązane do przestrzegania przepisów w zakresie ochrony danych mających zastosowanie do przetwarzania przez nie danych osobowych w ramach wykonywania funkcji dotyczących PKI ESBC.

Artykuł 13

Audyt

Audyty PKI ESBC przeprowadza się zgodnie z zasadami i ustaleniami zawartymi w polityce audytu. Nie narusza to wewnętrznych kontroli i zasad audytu mających zastosowanie do banków centralnych Eurosystemu lub przez te banki ustanowionych.

Artykuł 14

Ustalenia finansowe

Banki centralne Eurosystemu ponoszą koszty stworzenia i obsługi PKI ESBC zgodnie ze szczegółowymi postanowieniami ram finansowych PKI ESBC.

Artykuł 15

Rola Zarządu

1. Zgodnie z art. 17 ust. 3 decyzji ECB/2004/2 z dnia 19 lutego 2004 r. przyjmującej Regulamin Europejskiego Banku Centralnego [1] Rada Prezesów przekazuje Zarządowi swoje kompetencje regulacyjne do podejmowania środków mających na celu wykonanie niniejszej decyzji, niezbędnych do zapewnienia efektywności i bezpieczeństwa PKI ESBC, oraz do przyjmowania zmian dotyczących technicznych aspektów PKI ESBC i usług PKI ESBC, o których mowa w załącznikach do umowy pomiędzy poziomami 2 i 3, po uwzględnieniu opinii Komitetu ESBC ds. Informatyki oraz, w odpowiednich przypadkach, Komitetu Sterującego Eurosystemu ds. Informatyki.

2. Zarząd niezwłocznie zawiadamia Radę Prezesów o wszelkich środkach podejmowanych zgodnie z ust. 1 i stosuje się do wszelkich decyzji wydanych w tym zakresie przez Radę Prezesów.

Sporządzono we Frankfurcie nad Menem dnia 11 stycznia 2013 r.

Mario DRAGHI

Prezes EBC

[1] Dz.U. L 80 z 18.3.2004, s. 33.

ZAŁĄCZNIK

Informacje dotyczące organu certyfikacji PKI ESBC, w tym jego tożsamości, oraz elementów technicznych

Organ certyfikacji PKI ESBC jest określony w swoim certyfikacie jako wydawca a jego prywatny klucz jest używany do podpisywania certyfikatów. Organ certyfikacji PKI ESBC jest właściwy w sprawach:

(i) wydawania certyfikatów klucza publicznego i prywatnego;

(ii) wydawania list unieważnionych certyfikatów;

(iii) generowania par kluczy powiązanych z określonymi certyfikatami, np. tymi, które wymagają odtworzenia klucza;

(iv) ponoszenia ogólnej odpowiedzialności za PKI ESBC i zapewnienia spełniania wszelkich wymogów niezbędnych do jego działania.

Organ certyfikacji PKI ESBC obejmuje wszystkie osoby, polityki, procedury i systemy komputerowe, którym powierzono wydawanie certyfikatów elektronicznych i przypisywanie ich subskrybentom certyfikatów.

Organ certyfikacji PKI ESBC obejmuje dwa elementy techniczne:

— **Główny organ certyfikacji PKI ESBC (Root ESCB-PKI certification authority)**: ten organ certyfikacji, funkcjonujący na poziomie pierwszym, wydaje certyfikaty dla siebie oraz podlegających mu organów certyfikacji. Działa jedynie podczas wykonywania swoich wąsko zdefiniowanych zadań. Oto jego najważniejsze dane:

Distinguished name (identyfikator wyróżniający)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial numer (numer seryjny)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Distinguished name of issuer (identyfikator wyróżniający wydawcy)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (okres ważności)	From 21-06-2011 11:58:26 to 21-06-2041 11:58:26
Message digest (SHA-1) (streszczenie wiadomości)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192

— **Organ certyfikacji PKI ESBC on-line (Online ESCB-PKI certification authority)**: ten organ certyfikacji, funkcjonujący na poziomie drugim, podlega głównemu organowi certyfikacji PKI ESBC. Odpowiada on za wydawanie certyfikatów PKI ESBC użytkownikom. Oto jego najważniejsze dane:

Distinguished name (identyfikator wyróżniający)	CN=ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial numer (numer seryjny)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished name of issuer (identyfikator wyróżniający wydawcy)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (okres ważności)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (SHA-1) (streszczenie wiadomości)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08