DECYZJE

DECYZJA EUROPEJSKIEGO BANKU CENTRALNEGO (UE) 2016/187

z dnia 11 grudnia 2015 r.

zmieniająca decyzję EBC/2013/1 ustanawiającą ramy infrastruktury klucza publicznego Europejskiego Systemu Banków Centralnych (EBC/2015/46)

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, w szczególności art. 12 ust. 1 w związku z art. 3 ust. 1, art. 5, art. 12 ust. 3 oraz art. 16, art. 24 i art. 34,

a także mając na uwadze, co następuje:

(1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([1]) uchyliło dyrektywę 1999/93/WE Parlamentu Europejskiego i Rady ([2]) ze skutkiem od dnia 1 lipca 2016 r. Decyzja EBC/2013/1 powinna zatem odsyłać do rozporządzenia (UE) nr 910/2014 ([3]).

(2) Zawarte w załączniku do decyzji ECB/2013/1 informacje dotyczące organu certyfikacji PKI ESBC, w tym jego tożsamości oraz elementów technicznych, wymagają aktualizacji.

(3) Decyzja EBC/2013/1 powinna zatem zostać odpowiednio zmieniona,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Zmiany

W decyzji EBC/2013/1 wprowadza się następujące zmiany:

1) artykuł 1 pkt 10 otrzymuje brzmienie:

„10. »organ certyfikacji PKI ESBC« – podmiot, który jest zaufanym podmiotem użytkowników w zakresie wydawania, unieważniania i odnawiania certyfikatów PKI ESBC lub zarządza nimi zgodnie z zasadami akceptacji certyfikatów ESBC/SSM;";

2) artykuł 4 ust. 4 otrzymuje brzmienie:

„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

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

([2]) Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.U. L 13 z 19.1.2000, s. 12).

([3]) Decyzja Europejskiego Banku Centralnego EBC/2013/1 z dnia 11 stycznia 2013 r. ustanawiająca ramy infrastruktury klucza publicznego Europejskiego Systemu Banków Centralnych (Dz.U. L 74 z 16.3.2013, s. 30).

objętych zakresem dyrektywy 1999/93/WE i rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 (*), jak i certyfikatów elektronicznych nieobjętych zakresem tych aktów. 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.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).";

3) w art. 10 ust. 1 zdanie wprowadzające oraz lit. a) otrzymują brzmienie:

„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 i rozporządzenia (UE) nr 910/2014, 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 i rozporządzeniem (UE) nr 910/2014;";

4) załącznik otrzymuje brzmienie określone w załączniku do niniejszej decyzji.

Artykuł 2

Wejście w życie

Niniejsza decyzja wchodzi w życie trzeciego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono we Frankfurcie nad Menem dnia 11 grudnia 2015 r.

Mario DRAGHI

Prezes EBC

ZAŁĄCZNIK

„ZAŁĄCZNIK

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

a) Certyfikat SHA-1 ([1]):

Distinguished name (identyfikator wyróżniający)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (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
Message digest (SHA-256) (streszczenie wiadomości)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Cryptographic algorithms (algorytmy kryptograficzne)	SHA-1/RSA 4096

b) Certyfikat SHA-256:

Distinguished name (identyfikator wyróżniający)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (numer seryjny)	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8

([1]) Certyfikat wykorzystywany jedynie w systemach nie obsługujących wyższych algorytmów.

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 12:35:34 to 21-06-2041 12:35:34
Message digest (SHA-1) (streszczenie wiadomości)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message digest (SHA-256) (streszczenie wiadomości)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Cryptographic algorithms (algorytmy kryptograficzne)	SHA-256/RSA 4096

— **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:

a) Certyfikat SHA-1 ([1]):

Distinguished name (identyfikator wyróżniający)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (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
Message digest (SHA-256) (streszczenie wiadomości)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Cryptographic algorithms (algorytmy kryptograficzne)	SHA-1/RSA 4096

b) Certyfikat SHA-256:

Distinguished name (identyfikator wyróżniający)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (numer seryjny)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
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)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message digest (SHA-256) (streszczenie wiadomości)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Cryptographic algorithms (algorytmy kryptograficzne)	SHA-256/RSA 4096”

([1]) Certyfikat wykorzystywany jedynie w systemach nieobsługujących wyższych algorytmów.