DECISIONI

DECISIONE (UE) 2016/187 DELLA BANCA CENTRALE EUROPEA

dell'11 dicembre 2015

che modifica la Decisione BCE/2013/1 che definisce l'infrastruttura a chiavi pubbliche del Sistema europeo di banche centrali (BCE/2015/46)

IL CONSIGLIO DIRETTIVO DELLA BANCA CENTRALE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 127,

visto lo statuto del Sistema europeo di banche centrali e della Banca centrale europea, in particolare l'articolo 12.1, in combinato disposto con gli articoli 3.1, 5 e 12.3 e gli articoli 12.3, da 16 a 24 e 34,

considerando quanto segue:

(1) Il Regolamento (UE) n. 910/2004 del Parlamento europeo e del Consiglio ([1]) ha abrogato la Direttiva 1999/93/CE del Parlamento europeo e del Consiglio ([2]) con effetto dal 1º luglio 2016. Pertanto, nella Decisione BCE/2013/1 ([3]) è opportuno fare riferimento al Regolamento (UE) n. 910/2014.

(2) È necessario aggiornare le informazioni concernenti l'ente certificatore del PKI-SEBC, ivi inclusa la sua identità e le sue componenti tecniche, di cui all'allegato alla Decisione BCE/2013/1.

(3) Pertanto, è opportuno modificare la Decisione BCE/2013/1 di conseguenza,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Modifiche

La Decisione BCE/2013/1 è modificata come segue:

1. All'articolo 1, il punto 10 è sostituito dal seguente:

   «10. per "ente certificatore del PKI-SEBC" si intende l'ente riconosciuto dagli utenti per l'emissione, la gestione, la revoca e il rinnovo dei certificati PKI-SEBC conformemente alla disciplina del SEBC/SSM in materia di accreditamento dei certificati;»;

2. All'articolo 4, il paragrafo 4 è sostituito dal seguente:

   «4. Il manuale operativo per la certificazione PKI-SEBC è un insieme di regole che disciplina la vita dei certificati elettronici, dalla richiesta iniziale alla concessione o alla revoca, nonché le relazioni tra i richiedenti e i titolari, l'ente certificatore del PKI-SEBC e gli altri destinatari del servizio di certificazione. Il manuale disciplina i certificati elettronici che ricadono nell'ambito di applicazione della direttiva 1999/93/CE e del Regolamento (UE) N. 910/2014

([1]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (GU L 257 del 28.8.2014, pag. 73).
([2]) Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche (GU L 13 del 19.1.2000, pag. 12).
([3]) Decisione BCE/2013/1 della Banca centrale europea, dell'11 gennaio 2013, che definisce l'infrastruttura a chiavi pubbliche del Sistema europeo di banche centrali (GU L 74, del 16.3.2013, p. 30).

del Parlamento europeo e del Consiglio (*), nonché i certificati al di fuori di tale ambito. Esso dispone pure i ruoli e i compiti di tutte le parti e stabilisce le procedure relative all'emissione e alla gestione dei certificati. È allegato all'accordo tra livello 2 e livello 3.

(*) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la Direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).»;

3. all'articolo 10, la dichiarazione introduttiva e la lettera a) del paragrafo 1 sono sostituiti dai seguenti:

«1 Salvo che provino di non avere agito con negligenza, le banche centrali dell'Eurosistema sono responsabili conformemente alle proprie funzioni e ai propri compiti nel PKI-SEBC per ogni danno causato a un utente che faccia ragionevole affidamento su un certificato qualificato, come definito nella Direttiva 1999/93/CE e nel Regolamento (UE) N. 910/2014, relativamente a quanto segue:

a) per quanto riguarda l'esattezza, al momento del rilascio, di tutte le informazioni contenute nel certificato qualificato e il fatto che esso contenga tutti i dati prescritti per i certificati qualificati, secondo la definizione di cui alla direttiva 1999/93/CE e al Regolamento (UE) N. 910/2014;»;

4. l'allegato è sostituito dall'allegato alla presente decisione.

Articolo 2

Entrata in vigore

La presente decisione entra in vigore il terzo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Francoforte sul Meno, l'11 dicembre 2015

Il Presidente della BCE
Mario DRAGHI

ALLEGATO

«ALLEGATO

Informazioni relative all'ente certificatore del PKI-SEBC, ivi inclusa la sua identità, e le sue componenti tecniche

L'ente certificatore del PKI-SEBC è identificato nel proprio certificato come l'emittente e la sua chiave privata è usata per firmare i certificati. L'ente certificatore del PKI-SEBC è incaricato di:

i) emettere i certificati a chiave privata e pubblica;

ii) emettere le liste di revoca;

iii) generare coppie di chiavi associate a certificati specifici, quali quelli che richiedono una chiave di recupero;

iv) provvedere alle responsabilità generali connesse al PKI-SEBC e garantire che tutti i requisiti necessari per gestirlo siano soddisfatti.

L'ente certificatore del PKI-SEBC comprende tutte le persone, le politiche, le procedure e i sistemi informatici cui è affidata l'emissione di certificati elettronici e la loro assegnazione ai titolari di certificati.

L'ente certificatore del PKI-SEBC comprende due componenti tecniche:

— **L'ente certificatore Root ESCB-PKI:** Tale ente certificatore, di primo livello, emette solo certificati per se stesso e per gli enti certificatori ad esso subordinati. È operativo solo quando svolge i suoi compiti così strettamente definiti. I suoi dati più significativi sono i seguenti:

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

Distinguished name (Nome caratteristico)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (Codice seriale)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Distinguished name of issuer (Nome caratteristico dell'emittente)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (Periodo di validità)	From 21-06-2011 11:58:26 to 21-06-2041 11:58:26
Message digest (Valore di hash) (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Message digest (Valore di hash) (SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Cryptographic algorithms (Algoritmi crittografici)	SHA-1/RSA 4096

b) certificato SHA-256:

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

([1]) Tale certificato sarà utilizzato solo in sistemi che non supportano algoritmi di livello superiore.

Nome caratteristico dell'emittente (Distinguished name of issuer)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (Periodo di validità)	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
Message digest (Valore di hash) (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message digest (Valore di hash) (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Cryptographic algorithms (Algoritmi crittografici)	SHA-256/RSA 4096

— **L'ente certificatore ESCB-PKI online:** Tale ente certificatore, di secondo livello, è subordinato rispetto all'ente certificatore Root ESCB-PKI. È responsabile per l'emissione di certificati PKI-SEBC per gli utenti. I suoi dati più significativi sono i seguenti:

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

Distinguished name (Nome caratteristico)	CN = ESCB-PKI ONLINE CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (Codice seriale)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished name of issuer (Nome caratteristico dell'emittente)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Periodo di valdità (Validity period)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Valore di hash (Message digest) (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Valore di hash (Message digest) (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Algoritmi crittografici (Cryptographic algorithms)	SHA-1/RSA 4096

b) SHA-256 certificate:

Nome caratteristico (Distinguished name)	CN = ESCB-PKI ONLINE CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Codice seriale (Serial number)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Nome caratteristico dell'emittente (Distinguished name of issuer)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Periodo di valdità (Validity period)	Dal 22-07-2011 12:46:35 al 22-07-2026 12:46:35
Valore di hash (Message digest) (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Valore di hash (Message digest) (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Algoritmi crittografici (Cryptographic algorithms)	SHA-256/RSA 4096»

([1]) Tale certificato sarà utilizzato solo in sistemi che non supportano algoritmi di livello superiore.