ΑΠΟΦΑΣΕΙΣ

ΑΠΟΦΑΣΗ (ΕΕ) 2016/187 ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΕΝΤΡΙΚΗΣ ΤΡΑΠΕΖΑΣ

της 11ης Δεκεμβρίου 2015

που τροποποιεί την απόφαση ΕΚΤ/2013/1 για τη θέσπιση του πλαισίου της υποδομής δημόσιου κλειδιού για το Ευρωπαϊκό Σύστημα Κεντρικών Τραπεζών (ΕΚΤ/2015/46)

ΤΟ ΔΙΟΙΚΗΤΙΚΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΕΝΤΡΙΚΗΣ ΤΡΑΠΕΖΑΣ,

Έχοντας υπόψη τη συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 127,

Έχοντας υπόψη το καταστατικό του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών και της Ευρωπαϊκής Κεντρικής Τράπεζας, και ιδίως το άρθρο 12.1, σε συνδυασμό με τα άρθρα 3.1, 5, 12.3, 16 έως 24 και 34,

Εκτιμώντας τα ακόλουθα:

(1) Ο κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [1] κατήργησε την οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [2] από 1ης Ιουλίου 2016. Ως εκ τούτου, η απόφαση ΕΚΤ/2013/1 [3] ενδείκνυται να αναφέρεται στον κανονισμό (ΕΕ) αριθ. 910/2014.

(2) Οι πληροφορίες του παραρτήματος της απόφασης ΕΚΤ/2013/1 που αφορούν την αρχή πιστοποίησης ESCB-PKI, την ταυτότητα και τα τεχνικά υποσυστήματά της, χρήζουν ενημέρωσης.

(3) Ως εκ τούτου, η απόφαση ΕΚΤ/2013/1 θα πρέπει να τροποποιηθεί αναλόγως,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Τροποποιήσεις

Η απόφαση ΕΚΤ/2013/1 τροποποιείται ως εξής:

1) στο άρθρο 1, το σημείο 10 αντικαθίσταται από το ακόλουθο κείμενο:

«10. "αρχή πιστοποίησης ESCB-PKI": η οντότητα, την οποία εμπιστεύονται οι χρήστες για την έκδοση, διαχείριση, ανάκληση και ανανέωση των πιστοποιητικών της ESCB-PKI σύμφωνα με το πλαίσιο αποδοχής πιστοποιητικών του ΕΣΚΤ/ΕΕΜ·»·

2) στο άρθρο 4, η παράγραφος 4 αντικαθίσταται από το ακόλουθο κείμενο:

«4. Η δήλωση διαδικασιών πιστοποίησης της ESCB-PKI αποτελεί μια δέσμη κανόνων οι οποίοι διέπουν τον κύκλο ζωής των ψηφιακών πιστοποιητικών, από την αρχική αίτηση έκδοσής τους έως τη λήξη ή την ανάκλησή τους, καθώς και τις σχέσεις μεταξύ του αιτούντος την έκδοση πιστοποιητικού ή του κατόχου πιστοποιητικού, της αρχής πιστοποίησης ESCB-PKI και των οντοτήτων που βασίζονται σε πιστοποιητικό. Καλύπτει πιστοποιητικά εντός και εκτός του πεδίου εφαρμογής της

[1] Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ (ΕΕ L 257 της 28.8.2014, σ. 73).

[2] Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές (ΕΕ L 13 της 19.1.2000, σ. 12).

[3] Απόφαση ΕΚΤ/2013/1 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 11ης Ιανουαρίου 2013, για τη θέσπιση του πλαισίου της υποδομής δημόσιου κλειδιού για το Ευρωπαϊκό Σύστημα Κεντρικών Τραπεζών (ΕΕ L 74 της 16.3.2013, σ. 30).

οδηγίας 1999/93/ΕΚ και του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (*). Καθορίζει επίσης τα καθήκοντα και τις αρμοδιότητες όλων των συμβαλλομένων μερών και θεσπίζει τις διαδικασίες που αφορούν την έκδοση και διαχείριση των πιστοποιητικών. Αποτελεί παράρτημα της συμφωνίας επιπέδου 2 — επιπέδου 3.

(*) Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ (ΕΕ L 257 της 28.8.2014, σ. 73).»·

3) στο άρθρο 10, το πρώτο εδάφιο της παραγράφου 1 και το στοιχείο α) αυτής αντικαθίσταται από το ακόλουθο κείμενο:

«1. Εκτός εάν αποδείξουν ότι δεν ενήργησαν αμελώς, οι κεντρικές τράπεζες του Ευρωσυστήματος ευθύνονται βάσει των καθηκόντων και αρμοδιοτήτων τους στην ESCB-PKI για κάθε ζημία που προκλήθηκε σε χρήστη ο οποίος ευλόγως βασίζεται σε αναγνωρισμένο πιστοποιητικό, σύμφωνα με τους ορισμούς της οδηγίας 1999/93/ΕΚ και του κανονισμού (ΕΕ) αριθ. 910/2014, όσον αφορά:

α) την ακρίβεια όλων των πληροφοριών που περιέχονται σε αναγνωρισμένο πιστοποιητικό κατά το χρόνο έκδοσής του και το ερώτημα εάν το πιστοποιητικό περιέχει όλες τις λεπτομέρειες που απαιτούνται για ένα αναγνωρισμένο πιστοποιητικό, σύμφωνα με τους ορισμούς της οδηγίας 1999/93/ΕΚ και του κανονισμού (ΕΕ) αριθ. 910/2014·»·

4) το παράρτημα αντικαθίσταται από το παράρτημα της παρούσας απόφασης.

Άρθρο 2

Έναρξη ισχύος

Η παρούσα απόφαση αρχίζει να ισχύει την τρίτη ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Φρανκφούρτη, 11 Δεκεμβρίου 2015.

Ο Πρόεδρος της ΕΚΤ
Mario DRAGHI

ΠΑΡΑΡΤΗΜΑ

«ΠΑΡΑΡΤΗΜΑ

Πληροφορίες που αφορούν την αρχή πιστοποίησης ESCB-PKI, την ταυτότητα και τα τεχνικά υποσυστήματά της

Η αρχή πιστοποίησης ESCB-PKI αναγνωρίζεται στα πιστοποιητικά της ως εκδότης αυτών. Το ιδιωτικό κλειδί της χρησιμοποιείται για την υπογραφή των πιστοποιητικών. Η αρχή πιστοποίησης ESCB-PKI είναι επιφορτισμένη με:

i) την έκδοση πιστοποιητικών ιδιωτικού και δημόσιου κλειδιού·

ii) την έκδοση καταλόγων ανακληθέντων πιστοποιητικών·

iii) τη δημιουργία ζευγών κλειδιών που σχετίζονται με συγκεκριμένα πιστοποιητικά, π.χ. εκείνων που απαιτούν την ανάκτηση κλειδιού·

iv) την ανάληψη της συνολικής ευθύνης για την ESCB-PKI και τη διασφάλιση της τήρησης όλων των αναγκαίων απαιτήσεων για τη λειτουργία της.

Η αρχή πιστοποίησης ESCB-PKI περιλαμβάνει όλα τα άτομα, τις πολιτικές, τις διαδικασίες και τα συστήματα ψηφιακών πιστοποιητικών τα οποία είναι επιφορτισμένα με την έκδοση ψηφιακών πιστοποιητικών και τη χορήγησή τους στους κατόχους πιστοποιητικών.

Η αρχή πιστοποίησης ESCB-PKI περιλαμβάνει δύο τεχνικά υποσυστήματα:

— **Την κεντρική αρχή πιστοποίησης ESCB-PKI:** Η εν λόγω αρχή πιστοποίησης, σε πρώτο επίπεδο, εκδίδει πιστοποιητικά μόνο για δική της χρήση και για τις αρχές πιστοποίησης που υπάγονται σε αυτή. Λειτουργεί μόνον όταν εκτελεί τις αυστηρά καθορισμένες αρμοδιότητές της. Τα πιο σημαντικά στοιχεία της είναι τα εξής:

α) Πιστοποιητικό SHA-1 ([1]):

Διακεκριμένο όνομα (Distinguished name)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Αύξων αριθμός (Serial number)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Διακεκριμένο όνομα εκδότη (Distinguished name of Issuer)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Περίοδος ισχύος (Validity period)	Από 21-06-2011 11:58:26 έως 21-06-2041 11:58:26
Περίληψη μηνύματος (Message Digest) (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Περίληψη μηνύματος (Message Digest) (SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Κρυπτογραφικοί αλγόριθμοι	SHA-1/RSA 4096

β) Πιστοποιητικό SHA-256:

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

([1]) Το πιστοποιητικό αυτό θα χρησιμοποιείται μόνο σε συστήματα που δεν υποστηρίζουν υψηλότερους αλγόριθμους.

Διακεκριμένο όνομα εκδότη (Distinguished name of Issuer)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Περίοδος ισχύος (Validity period)	Από 21-06-2011 12:35:34 μμ έως 21-06-2041 12:35:34 μμ
Περίληψη μηνύματος (Message Digest) (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Περίληψη μηνύματος (Message Digest) (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Κρυπτογραφικοί αλγόριθμοι	SHA-256/RSA 4096

— **Την online αρχή πιστοποίησης ESCB-PKI:** Η εν λόγω αρχή πιστοποίησης, σε δεύτερο επίπεδο, υπάγεται στην κεντρική αρχή πιστοποίησης ESCB-PKI. Είναι υπεύθυνη για την έκδοση πιστοποιητικών της ESCB-PKI για χρήστες. Τα πιο σημαντικά στοιχεία της είναι τα εξής:

α) Πιστοποιητικό SHA-1 ([1]):

Διακεκριμένο όνομα (Distinguished name)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Αύξων αριθμός (Serial number)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Διακεκριμένο όνομα εκδότη (Distinguished name of Issuer)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Περίοδος ισχύος (Validity period)	Από 22-07-2011 12:46:35 μμ έως 22-07-2026 12:46:35 μμ
Περίληψη μηνύματος (Message Digest) (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Περίληψη μηνύματος (Message Digest) (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Κρυπτογραφικοί αλγόριθμοι	SHA-1/RSA 4096

β) Πιστοποιητικό SHA-256:

Διακεκριμένο όνομα (Distinguished name)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Αύξων αριθμός (Serial number)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Διακεκριμένο όνομα εκδότη (Distinguished name of Issuer)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Περίοδος ισχύος (Validity period)	Από 22-07-2011 12:46:35 μμ έως 22-07-2026 12:46:35 μμ
Περίληψη μηνύματος (Message Digest) (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Περίληψη μηνύματος (Message Digest) (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Κρυπτογραφικοί αλγόριθμοι	SHA-256/RSA 4096»

([1]) Το πιστοποιητικό αυτό θα χρησιμοποιείται μόνο σε συστήματα που δεν υποστηρίζουν υψηλότερους αλγόριθμους.