Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2024/3144

19.12.2024

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/3144 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 18ης Δεκεμβρίου 2024

για την τροποποίηση του εκτελεστικού κανονισμού (ΕΕ) 2024/482 όσον αφορά τα εφαρμοστέα διεθνή πρότυπα και για τη διόρθωση του εν λόγω εκτελεστικού κανονισμού

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) ([1]), και ιδίως το άρθρο 49 παράγραφος 7,

Εκτιμώντας τα ακόλουθα:

(1) Με τον εκτελεστικό κανονισμό (ΕΕ) 2024/482 της Επιτροπής ([2]) προσδιορίζονται οι ρόλοι, οι κανόνες και οι υποχρεώσεις, καθώς και η δομή του βασισμένου σε κοινά κριτήρια ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας (EUCC), σύμφωνα με το ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας που περιγράφεται στον κανονισμό (ΕΕ) 2019/881.

(2) Ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 βασίζεται σε καθιερωμένα διεθνή πρότυπα, τα οποία είναι τα κοινά κριτήρια και η κοινή μεθοδολογία αξιολόγησης που τηρούν ο Διεθνής Οργανισμός Τυποποίησης (ISO) και η Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC). Ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 παραπέμπει σε πρότυπα ISO/IEC, αλλά δεν προσδιορίζει την εφαρμοστέα έκδοση των εν λόγω προτύπων. Ως εκ τούτου, θα πρέπει να διευκρινιστεί ποια έκδοση των προτύπων ισχύει για τα πιστοποιητικά που εκδίδονται στο πλαίσιο του EUCC.

(3) Οι κυβερνητικοί οργανισμοί που συνέβαλαν στην κατάρτιση των κοινών κριτηρίων και της κοινής μεθοδολογίας αξιολόγησης μέσω της ρύθμισης για την αναγνώριση των πιστοποιητικών κοινών κριτηρίων στον τομέα της ασφάλειας ΤΠ (CCRA) είναι από κοινού κάτοχοι, μαζί με τον ISO / την IEC, των δικαιωμάτων πνευματικής ιδιοκτησίας επί των εγγράφων αυτών. Οι εν λόγω κυβερνητικοί οργανισμοί διατηρούν το δικαίωμα χρήσης των εγγράφων αυτών. Λαμβανομένης δε υπόψη της σημασίας που έχουν τα εν λόγω έγγραφα που προέκυψαν από τη CCRA, θα πρέπει επίσης να αποτελούν τη βάση για την πιστοποίηση στο πλαίσιο του EUCC.

(4) Τα πρότυπα κοινών κριτηρίων και κοινής μεθοδολογίας αξιολόγησης υπόκεινται σε ερμηνείες από τη CCRA, οι οποίες διευκολύνουν την εφαρμογή τους και οι οποίες μπορούν να λαμβάνονται υπόψη από τις εγκαταστάσεις αξιολόγησης της ασφάλειας της τεχνολογίας πληροφοριών (ΕΑΑΤΠ) και τους οργανισμούς πιστοποίησης.

(5) Τα διεθνή πρότυπα που αφορούν τα κοινά κριτήρια ενδέχεται να υπόκεινται σε επικαιροποιήσεις. Για να διασφαλιστεί η ομαλή και έγκαιρη μετάβαση, είναι σκόπιμο να καθοριστούν μεταβατικοί κανόνες, ώστε να δοθεί στους πωλητές, στις ΕΑΑΤΠ και στους οργανισμούς πιστοποίησης, καθώς και σε άλλους σχετικούς φορείς, επαρκής χρόνος για τις αναγκαίες προσαρμογές. Οι εν λόγω μεταβατικοί κανόνες θα πρέπει να ευθυγραμμίζονται στον κατάλληλο βαθμό με τις παγκόσμιες πρακτικές, όπως αυτές που καθορίζονται από τη CCRA.

([1]) ΕΕ L 151 της 7.6.2019, σ. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής, της 31ης Ιανουαρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την έγκριση του ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (EUCC) (ΕΕ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(6) Ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 δεν προσδιορίζει μέχρι πότε η πιστοποίηση προϊόντων ΤΠΕ μπορεί να βασίζεται στις προηγούμενες εκδόσεις των προτύπων κοινών κριτηρίων και κοινής μεθοδολογίας αξιολόγησης. Οι τεχνικοί τομείς και τα χαρακτηριστικά προστασίας που παρατίθενται στα παραρτήματα I, II και III του εν λόγω εκτελεστικού κανονισμού βασίζονται σε προηγούμενες εκδόσεις των προτύπων ISO/IEC 15408 και 18045. Ως εκ τούτου, ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 θα πρέπει να προσδιορίζει, αφενός, υπό ποιες συνθήκες εξακολουθεί να ισχύει η προηγούμενη έκδοση των κοινών κριτηρίων και της κοινής μεθοδολογίας αξιολόγησης και, αφετέρου, τον τρόπο με τον οποίο θα πραγματοποιηθεί η μετάβαση στην τελευταία έκδοση των διεθνών προτύπων.

(7) Κατά τη διάρκεια της μεταβατικής περιόδου, η επικαιροποίηση των σχετικών τεχνικών τομέων και χαρακτηριστικών προστασίας θα πρέπει να αποτελεί προτεραιότητα για τα σχετικά ενδιαφερόμενα μέρη. Ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 θα πρέπει να προβλέπει ότι οι στόχοι ασφάλειας που βασίζονται σε προηγούμενη έκδοση των προτύπων θα γίνονται αποδεκτοί έως την 31η Δεκεμβρίου 2027 σύμφωνα με την πολιτική μετάβασης που έχει εγκρίνει η CCRA. Ωστόσο, πρέπει να σημειωθεί ότι η πολιτική μετάβασης της CCRA καλύπτει τις αρχικές αξιολογήσεις προϊόντων και χαρακτηριστικών προστασίας που ξεκίνησαν το αργότερο στις 30 Ιουνίου 2024, ημερομηνία κατά την οποία το EUCC δεν είχε τεθεί ακόμη σε εφαρμογή. Επιπλέον, σύμφωνα με την πολιτική μετάβασης της CCRA, ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 θα πρέπει να προβλέπει ότι οι στόχοι ασφάλειας που συμμορφώνονται προς τον εν λόγω εκτελεστικό κανονισμό με δήλωση συμμόρφωσης προς χαρακτηριστικά προστασίας που βασίζονται σε προηγούμενη έκδοση των προτύπων θα γίνονται αποδεκτοί έως την 31η Δεκεμβρίου 2027. Επιπλέον, όταν εκδίδεται νέο πιστοποιητικό δυνάμει του εκτελεστικού κανονισμού (ΕΕ) 2024/482 στο πλαίσιο διαδικασίας επανεξέτασης εθνικού πιστοποιητικού η οποία αρχίζει εντός δύο ετών από την έκδοση του αρχικού πιστοποιητικού, θα πρέπει να είναι δυνατή η χρήση προηγούμενης έκδοσης των προτύπων. Αυτό δεν αφορά την περίπτωση διαδικασίας επανεξέτασης που δεν απαιτεί την έκδοση νέου πιστοποιητικού σύμφωνα με τον εκτελεστικό κανονισμό (ΕΕ) 2024/482 και όπου το πιστοποιητικό παραμένει σε ισχύ.

(8) Προκειμένου να διασφαλίζεται η ομαλή μετάβαση στην τελευταία έκδοση των προτύπων, ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 θα πρέπει να προβλέπει ειδικούς μεταβατικούς κανόνες και να συνεχίσει να επιτρέπει την έκδοση πιστοποιητικών βάσει του εν λόγω εκτελεστικού κανονισμού με δήλωση συμμόρφωσης προς χαρακτηριστικά προστασίας τα οποία βασίζονται σε προηγούμενες εκδόσεις των προτύπων που έχει δημοσιεύσει η CCRA, όταν η χρήση των εν λόγω χαρακτηριστικών προστασίας απαιτείται βάσει της ενωσιακής νομοθεσίας. Εν προκειμένω, νοούνται ο εκτελεστικός κανονισμός (ΕΕ) 2016/799 της Επιτροπής ([3]), καθώς και ο κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]) και η εκτελεστική απόφαση (ΕΕ) 2016/650 της Επιτροπής ([5]).

(9) Στο παράρτημα I του εκτελεστικού κανονισμού (ΕΕ) 2024/482 παρατίθενται τα εφαρμοστέα έγγραφα στάθμης της τεχνικής για την αξιολόγηση προϊόντων ΤΠΕ και χαρακτηριστικών προστασίας. Ωστόσο, δεν προσδιορίζεται η έκδοση των εγγράφων. Ως εκ τούτου, θα πρέπει να διευκρινιστεί ποια έκδοση των εγγράφων ισχύει για τα πιστοποιητικά που εκδίδονται στο πλαίσιο του EUCC. Οι εκδόσεις αυτές βασίζονται σε έγγραφα που έχουν εγκριθεί από την ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας (ΕΟΠΙΚ), ενώ έχουν υποβληθεί σε περαιτέρω επανεξέταση για την ενσωμάτωσή τους στο EUCC. Επιπλέον, το παράρτημα I θα πρέπει να τροποποιηθεί ώστε να συμπεριλάβει επικαιροποιημένα και νέα έγγραφα στάθμης της τεχνικής μετά την έγκρισή τους από την ΕΟΠΙΚ, διασφαλίζοντας με αυτόν τον τρόπο ενιαία διαπίστευση των οργανισμών αξιολόγησης της συμμόρφωσης στο πλαίσιο του EUCC. Οι απαιτήσεις διαπίστευσης που σχετίζονται με τη διαπίστευση των ΕΑΑΤΠ θα πρέπει να επικαιροποιηθούν ώστε να αποσαφηνιστεί η εφαρμογή των κριτηρίων ανεξαρτησίας και αμεροληψίας, ενώ επίσης θα πρέπει να καθιερωθεί νέο έγγραφο στάθμης της τεχνικής για τη διαπίστευση των οργανισμών πιστοποίησης.

(10) Έγγραφα στάθμης της τεχνικής μπορούν να προστίθενται στο EUCC ή να υπόκεινται σε επικαιροποιήσεις στο πλαίσιο των οικείων δραστηριοτήτων διατήρησης. Για νέα ή επικαιροποιημένα έγγραφα στάθμης της τεχνικής, ενδέχεται να χρειαστεί να θεσπιστούν κατάλληλοι μεταβατικοί κανόνες, ώστε να δοθεί η δυνατότητα στους πωλητές, στις ΕΑΑΤΠ, στους οργανισμούς πιστοποίησης και σε άλλα ενδιαφερόμενα μέρη να προβούν στις αναγκαίες προσαρμογές. Για την επικαιροποίηση του εγγράφου στάθμης της τεχνικής σχετικά με τη διαπίστευση των ΕΑΑΤΠ, το επικαιροποιημένο έγγραφο θα πρέπει να εφαρμόζεται στις διαπιστεύσεις που έχουν εκδοθεί πριν από τις 8 Ιουλίου 2025 μόνο όταν επανεξετάζονται, όπως π.χ. στο πλαίσιο διαδικασίας αξιολόγησης ή επαναξιολόγησης. Επιπλέον, το επικαιροποιημένο έγγραφο θα πρέπει να εφαρμόζεται σε όλες τις διαπιστεύσεις για ΕΑΑΤΠ οι οποίες έχουν εκδοθεί μετά τις 8 Ιουλίου 2025.

([3]) Εκτελεστικός κανονισμός (ΕΕ) 2016/799 της Επιτροπής, της 18ης Μαρτίου 2016, σχετικά με την εφαρμογή του κανονισμού (ΕΕ) αριθ. 165/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, ο οποίος καθορίζει τις απαιτήσεις κατασκευής, δοκιμής, εγκατάστασης, λειτουργίας και επισκευής ταχογράφων και των δομικών στοιχείων τους (ΕΕ L 139 της 26.5.2016, σ. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Εκτελεστική απόφαση (ΕΕ) 2016/650 της Επιτροπής, της 25ης Απριλίου 2016, σχετικά με τον καθορισμό προτύπων για την αξιολόγηση της ασφάλειας των εγκεκριμένων διατάξεων δημιουργίας υπογραφής και σφραγίδας σύμφωνα με το άρθρο 30 παράγραφος 3 και το άρθρο 39 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (ΕΕ L 109 της 26.4.2016, σ. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Περαιτέρω διορθώσεις στα άρθρα 5, 8, 16, 29 και 44 και στο παράρτημα IV του εκτελεστικού κανονισμού (ΕΕ) 2024/482 συμβάλλουν στη διασφάλιση ομοιόμορφης διατύπωσης και σαφούς νομικής ερμηνείας.

(12) Οι κανόνες για τις κοινοποιήσεις των οργανισμών αξιολόγησης της συμμόρφωσης θα πρέπει να θεσπιστούν με οριζόντιο τρόπο για όλα τα σχήματα που εντάσσονται στο ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας. Ο εκτελεστικός κανονισμός (ΕΕ) 2024/3143 της Επιτροπής ([6]) καλύπτει τους εν λόγω κανόνες κοινοποίησης. Ως εκ τούτου, τα άρθρα 23 και 24 του εκτελεστικού κανονισμού (ΕΕ) 2024/482 θα πρέπει να απαλειφθούν από την ημερομηνία εφαρμογής του εκτελεστικού κανονισμού 2024/3143.

(13) Συνεπώς, ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 θα πρέπει να τροποποιηθεί και να διορθωθεί αναλόγως.

(14) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 66 του κανονισμού (ΕΕ) 2019/881,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 τροποποιείται ως εξής:

1) στο άρθρο 2, τα σημεία 1) και 2) αντικαθίστανται από το ακόλουθο κείμενο:

«1) "κοινά κριτήρια": τα κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, τα οποία καθορίζονται στα πρότυπα ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 ή ISO/IEC 15408-5:2022, ή καθορίζονται στα κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, έκδοση CC:2022, μέρη 1 έως 5, που δημοσιεύθηκαν από τους συμμετέχοντες στη ρύθμιση για την αναγνώριση των πιστοποιητικών κοινών κριτηρίων στον τομέα της ασφάλειας ΤΠ·

2) "κοινή μεθοδολογία αξιολόγησης": η κοινή μεθοδολογία για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, η οποία καθορίζεται στο πρότυπο ISO/IEC 18045:2022, ή η κοινή μεθοδολογία για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, έκδοση CEM:2022, που δημοσιεύθηκε από τους συμμετέχοντες στη ρύθμιση για την αναγνώριση των πιστοποιητικών κοινών κριτηρίων στον τομέα της ασφάλειας ΤΠ·»·

2) το άρθρο 3 αντικαθίσταται από το ακόλουθο κείμενο:

«*Άρθρο 3*

Πρότυπα αξιολόγησης

1. Στις αξιολογήσεις που διενεργούνται στο πλαίσιο του σχήματος EUCC εφαρμόζονται τα ακόλουθα πρότυπα:

α) τα κοινά κριτήρια·

β) η κοινή μεθοδολογία αξιολόγησης.

2. Έως την 31η Δεκεμβρίου 2027, μπορούν να εκδίδονται πιστοποιητικά στο πλαίσιο του σχήματος EUCC με εφαρμογή ενός εκ των ακολούθων προτύπων:

α) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 ή ISO/IEC 15408-3:2008·

β) Κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, έκδοση 3.1, αναθεώρηση 5, που δημοσιεύθηκαν από τους συμμετέχοντες στη ρύθμιση για την αναγνώριση των πιστοποιητικών κοινών κριτηρίων στον τομέα της ασφάλειας ΤΠ·

([6]) Εκτελεστικός κανονισμός (ΕΕ) 2024/3143 της Επιτροπής, της 18ης Δεκεμβρίου 2024, για τον καθορισμό των συνθηκών, της μορφής και των διαδικασιών που ισχύουν για τις κοινοποιήσεις σύμφωνα με το άρθρο 61 παράγραφος 5 του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών (ΕΕ L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

γ) ISO/IEC 18045:2008·

δ) Κοινή μεθοδολογία για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, αναθεώρηση 5, έκδοση 3.1, που δημοσιεύθηκε από τους συμμετέχοντες στη ρύθμιση για την αναγνώριση των πιστοποιητικών κοινών κριτηρίων στον τομέα της ασφάλειας ΤΠ.

3. Έως την 31η Δεκεμβρίου 2027, μπορεί να εκδίδεται πιστοποιητικό στο πλαίσιο του σχήματος EUCC με εφαρμογή των προτύπων που αναφέρονται στην παράγραφο 1, με δήλωση συμμόρφωσης προς χαρακτηριστικό προστασίας στο οποίο έχουν εφαρμοστεί τα πρότυπα που παρατίθενται στην παράγραφο 2.

4. Πιστοποιητικό το οποίο εφαρμόζει τα πρότυπα που αναφέρονται στην παράγραφο 1 μπορεί επίσης να εκδίδεται στο πλαίσιο του σχήματος EUCC με δήλωση συμμόρφωσης προς χαρακτηριστικό προστασίας στο οποίο έχει εφαρμοστεί οποιοδήποτε από τα ακόλουθα πρότυπα, υπό την προϋπόθεση ότι η χρήση του εν λόγω χαρακτηριστικού προστασίας απαιτείται βάσει του εκτελεστικού κανονισμού (ΕΕ) 2016/799 της Επιτροπής (*), του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (**) ή της εκτελεστικής απόφασης (ΕΕ) 2016/650 της Επιτροπής (***):

α) Κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, έκδοση 3.1, αναθεώρηση 1 έως 4, που δημοσιεύθηκαν από τους συμμετέχοντες στη ρύθμιση για την αναγνώριση των πιστοποιητικών κοινών κριτηρίων στον τομέα της ασφάλειας ΤΠ·

β) Κοινή μεθοδολογία για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών, έκδοση 3.1, αναθεώρηση 1 έως 4, που δημοσιεύθηκε από τους συμμετέχοντες στη ρύθμιση για την αναγνώριση των πιστοποιητικών κοινών κριτηρίων στον τομέα της ασφάλειας ΤΠ.

_____

(*) Εκτελεστικός κανονισμός (ΕΕ) 2016/799 της Επιτροπής, της 18ης Μαρτίου 2016, σχετικά με την εφαρμογή του κανονισμού (ΕΕ) αριθ. 165/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, ο οποίος καθορίζει τις απαιτήσεις κατασκευής, δοκιμής, εγκατάστασης, λειτουργίας και επισκευής ταχογράφων και των δομικών στοιχείων τους (ΕΕ L 139 της 26.5.2016, σ. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) 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, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Εκτελεστική απόφαση (ΕΕ) 2016/650 της Επιτροπής, της 25ης Απριλίου 2016, σχετικά με τον καθορισμό προτύπων για την αξιολόγηση της ασφάλειας των εγκεκριμένων διατάξεων δημιουργίας υπογραφής και σφραγίδας σύμφωνα με το άρθρο 30 παράγραφος 3 και το άρθρο 39 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (ΕΕ L 109 της 26.4.2016, σ. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).»·

3) στο κεφάλαιο IV προστίθεται το ακόλουθο άρθρο 20α:

«Άρθρο 20α

Προσδιορισμός των απαιτήσεων για τη διαπίστευση οργανισμών αξιολόγησης της συμμόρφωσης

Για τη διαπίστευση των οργανισμών αξιολόγησης της συμμόρφωσης λαμβάνεται υπόψη ο προσδιορισμός των απαιτήσεων για τη διαπίστευση των οργανισμών πιστοποίησης και των ΕΑΑΤΠ, όπως προβλέπεται στα εφαρμοστέα έγγραφα στάθμης της τεχνικής που παρατίθενται στο σημείο 2 του παραρτήματος Ι.»·

4) τα άρθρα 23 και 24 απαλείφονται·

5) στο άρθρο 48 προστίθεται η ακόλουθη παράγραφος 4:

«4. Εκτός εάν ορίζεται διαφορετικά στο παράρτημα Ι ή ΙΙ, τα έγγραφα στάθμης της τεχνικής ισχύουν από την ημερομηνία εφαρμογής της τροποποιητικής πράξης με την οποία ενσωματώθηκαν στο παράρτημα Ι ή ΙΙ.»·

6) στο άρθρο 49 προστίθεται η ακόλουθη παράγραφος 4:

«4. Κατά τη διενέργεια της επανεξέτασης που αναφέρεται στην παράγραφο 3, εντός δύο ετών από την έκδοση του αρχικού πιστοποιητικού και όταν η εν λόγω επανεξέταση οδηγεί στην έκδοση νέου πιστοποιητικού σύμφωνα με τον παρόντα κανονισμό, μπορούν να εφαρμόζονται τα πρότυπα που παρατίθενται στο άρθρο 3 παράγραφος 2. Ως ημερομηνία έκδοσης του αρχικού πιστοποιητικού νοείται η ημερομηνία έκδοσης του τελευταίου πιστοποιητικού για προϊόν ΤΠΕ ή χαρακτηριστικό προστασίας στο οποίο βασίζεται η τρέχουσα πιστοποίηση.»·

7) το παράρτημα Ι αντικαθίσταται από το κείμενο του παραρτήματος Ι του παρόντος κανονισμού·

8) το παράρτημα IV τροποποιείται σύμφωνα με το παράρτημα ΙΙ του παρόντος κανονισμού.

Άρθρο 2

Ο εκτελεστικός κανονισμός (ΕΕ) 2024/482 διορθώνεται ως εξής:

1) στο άρθρο 5 παράγραφος 1, το στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) με δήλωση συμμόρφωσης προς πιστοποιημένο χαρακτηριστικό προστασίας στο πλαίσιο διαδικασίας ΤΠΕ, όταν το προϊόν ΤΠΕ εμπίπτει στην κατηγορία προϊόντων ΤΠΕ που καλύπτεται από το συγκεκριμένο χαρακτηριστικό προστασίας.»·

2) το άρθρο 8 διορθώνεται ως εξής:

α) ο τίτλος αντικαθίσταται από το ακόλουθο κείμενο:

«Απαραίτητες πληροφορίες για την πιστοποίηση και την αξιολόγηση»·

β) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Οι αιτούντες πιστοποίηση στο πλαίσιο του EUCC παρέχουν ή διαθέτουν με άλλον τρόπο στον οργανισμό πιστοποίησης και στην ΕΑΤΤΠ κάθε πληροφορία αναγκαία για τις δραστηριότητες πιστοποίησης και αξιολόγησης.»·

3) το άρθρο 16 αντικαθίσταται από το ακόλουθο κείμενο:

«*Άρθρο 16*

Απαραίτητες πληροφορίες για την πιστοποίηση και την αξιολόγηση χαρακτηριστικών προστασίας

Οι αιτούντες πιστοποίηση χαρακτηριστικού προστασίας στο πλαίσιο του EUCC παρέχουν ή διαθέτουν με άλλον τρόπο στον οργανισμό πιστοποίησης και στην ΕΑΤΤΠ κάθε πληροφορία αναγκαία για τις δραστηριότητες πιστοποίησης και αξιολόγησης σε πλήρη και ορθή μορφή. Το άρθρο 8 παράγραφοι 2, 3, 4 και 7 εφαρμόζεται τηρουμένων των αναλογιών.».

4) στο άρθρο 17, η παράγραφος 1 απαλείφεται·

5) στο άρθρο 29, η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

«2. Σε περίπτωση που ο κάτοχος του πιστοποιητικού EUCC δεν προτείνει κατάλληλα διορθωτικά μέτρα εντός της προθεσμίας που αναφέρεται στην παράγραφο 1, το πιστοποιητικό αναστέλλεται σύμφωνα με το άρθρο 30 ή ανακαλείται σύμφωνα με τα άρθρα 14 ή 20.».

Άρθρο 3

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Το άρθρο 1 σημείο 4) εφαρμόζεται από τις 8 Ιανουαρίου 2025.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 18 Δεκεμβρίου 2024.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

ΠΑΡΑΡΤΗΜΑ I

«ΠΑΡΑΡΤΗΜΑ I

Έγγραφα στάθμης της τεχνικής που υποστηρίζουν τεχνικούς τομείς και άλλα έγγραφα στάθμης της τεχνικής

1. Έγγραφα στάθμης της τεχνικής που υποστηρίζουν τεχνικούς τομείς σε επίπεδο AVA_VAN 4 ή 5:

   α) τα ακόλουθα έγγραφα σχετικά με την εναρμονισμένη αξιολόγηση του τεχνικού τομέα "έξυπνες κάρτες και παρεμφερείς διατάξεις":

      1) "Minimum ITSEF requirements for security evaluations of smart cards and similar devices" (Ελάχιστες απαιτήσεις ΕΑΑΤΠ για αξιολογήσεις ασφάλειας έξυπνων καρτών και παρεμφερών διατάξεων), έκδοση 1.1·

      2) "Minimum Site Security Requirements" (Ελάχιστες απαιτήσεις ασφάλειας χώρου), έκδοση 1.1·

      3) "Application of Common Criteria to integrated circuits" (Εφαρμογή κοινών κριτηρίων σε ολοκληρωμένα κυκλώματα), έκδοση 1.1·

      4) "Security Architecture requirements (ADV_ARC) for smart cards and similar devices" [Απαιτήσεις αρχιτεκτονικής ασφάλειας (ADV_ARC) για έξυπνες κάρτες και παρεμφερείς διατάξεις], έκδοση 1.1·

      5) "Certification of 'open' smart card products" (Πιστοποίηση "ανοικτών" προϊόντων έξυπνων καρτών), έκδοση 1.1·

      6) "Composite product evaluation for smart cards and similar devices" (Αξιολόγηση σύνθετων προϊόντων για έξυπνες κάρτες και παρεμφερείς διατάξεις), έκδοση 1.1·

      7) "Application of Attack Potential to Smartcards and Similar Devices" (Εφαρμογή κινδύνου επίθεσης σε έξυπνες κάρτες και παρεμφερείς διατάξεις), έκδοση 1.2·

   β) τα ακόλουθα έγγραφα σχετικά με την εναρμονισμένη αξιολόγηση του τεχνικού τομέα "διατάξεις υλισμικού με θυρίδες ασφαλείας":

      1) "Minimum ITSEF requirements for security evaluations of hardware devices with security boxes" (Ελάχιστες απαιτήσεις ΕΑΑΤΠ για αξιολογήσεις ασφάλειας διατάξεων υλισμικού με θυρίδες ασφαλείας), έκδοση 1.1·

      2) "Minimum Site Security Requirements" (Ελάχιστες απαιτήσεις ασφάλειας χώρου), έκδοση 1.1·

      3) "Application of Attack Potential to hardware devices with security boxes" (Εφαρμογή κινδύνου επίθεσης σε διατάξεις υλισμικού με θυρίδες ασφαλείας), έκδοση 1.2.

2. Έγγραφα στάθμης της τεχνικής σχετικά με την εναρμονισμένη διαπίστευση των οργανισμών αξιολόγησης της συμμόρφωσης:

   α) "Accreditation of ITSEFs for the EUCC" (Διαπίστευση ΕΑΑΤΠ για το EUCC), έκδοση 1.1 για διαπιστεύσεις που έχουν εκδοθεί πριν από τις 8 Ιουλίου 2025.

   β) "Accreditation of ITSEFs for the EUCC" (Διαπίστευση ΕΑΑΤΠ για το EUCC), έκδοση 1.6c, για διαπιστεύσεις που έχουν εκδοθεί για πρώτη φορά ή επανεξετάζονται μετά τις 8 Ιουλίου 2025.

   γ) "Accreditation of CBs for the EUCC" (Διαπίστευση οργανισμών πιστοποίησης για το EUCC), έκδοση 1.6b.»

ΠΑΡΑΡΤΗΜΑ ΙΙ

Στο παράρτημα IV του εκτελεστικού κανονισμού (ΕΕ) 2024/482, στο τμήμα IV.3, τα σημεία 5 και 6 αντικαθίστανται από το ακόλουθο κείμενο:

«5. Σε περίπτωση που οι αλλαγές έχουν επιβεβαιωθεί από τον οργανισμό πιστοποίησης ως ήσσονος σημασίας, δεν εκδίδεται νέο πιστοποιητικό για το τροποποιημένο προϊόν ΤΠΕ και εκπονείται έκθεση διατήρησης για την αρχική έκθεση πιστοποίησης.

Η έκθεση διατήρησης αποτελεί υποσύνολο της έκθεσης ανάλυσης επιπτώσεων και περιέχει τις ακόλουθες ενότητες:

α) εισαγωγή·

β) περιγραφή αλλαγών·

γ) επηρεαζόμενη τεκμηρίωση φορέα ανάπτυξης.

6. Η έκθεση διατήρησης που αναφέρεται στο σημείο 5 υποβάλλεται στον ENISA για δημοσίευση στον οικείο ιστότοπο πιστοποίησης της κυβερνοασφάλειας.».