Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/2532

17.12.2025

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/2532 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 16ης Δεκεμβρίου 2025

για τον καθορισμό κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τα πρότυπα αναφοράς και τις προδιαγραφές για τις εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (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 ([1]), και ιδίως το άρθρο 45ι παράγραφος 2,

Εκτιμώντας τα ακόλουθα:

(1) Με τον κανονισμό (ΕΕ) 2024/1183 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]), εισήχθη στον κανονισμό (ΕΕ) αριθ. 910/2014 κατάλογος νέων υπηρεσιών εμπιστοσύνης και εγκεκριμένων υπηρεσιών εμπιστοσύνης, συμπεριλαμβανομένης της εγκεκριμένης υπηρεσίας ηλεκτρονικής αρχειοθέτησης. Η Επιτροπή καλείται να καταρτίσει κατάλογο προτύπων αναφοράς και, όπου είναι απαραίτητο, να θεσπίσει προδιαγραφές για αυτές τις υπηρεσίες.

(2) Η ηλεκτρονική αρχειοθέτηση είναι υπηρεσία για την παραλαβή, αποθήκευση, ανάκτηση και διαγραφή ηλεκτρονικών δεδομένων και ηλεκτρονικών εγγράφων, ώστε να διασφαλίζεται η ανθεκτικότητα και η αναγνωσιμότητά τους και να διαφυλάσσεται η ακεραιότητα, η εμπιστευτικότητα και η απόδειξη της προέλευσής τους καθ' όλη τη διάρκεια της περιόδου διαφύλαξης. Οι εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης διαδραματίζουν καίριο ρόλο στο ψηφιακό επιχειρηματικό περιβάλλον, προωθώντας τη μετάβαση από τις παραδοσιακές έντυπες διαδικασίες σε ηλεκτρονικά ισοδύναμα. Για να διασφαλιστεί ότι τα ηλεκτρονικά δεδομένα και τα ηλεκτρονικά έγγραφα διαφυλάσσουν το τεκμήριο της ακεραιότητας και της προέλευσής τους κατά τη διάρκεια της περιόδου διαφύλαξης από τον εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης, και για να επιτευχθεί υψηλό επίπεδο διαφάνειας και εμπιστοσύνης μεταξύ όλων των συμμετεχόντων στον κύκλο ζωής των πληροφοριών, είναι αναγκαίο να θεσπιστεί ένα κοινό σύνολο προδιαγραφών για τις εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης.

(3) Για την αύξηση της αποδεικτικής αξίας, της ασφάλειας και της αξιοπιστίας των εγκεκριμένων υπηρεσιών ηλεκτρονικής αρχειοθέτησης, όταν χρησιμοποιούνται ηλεκτρονικές υπογραφές, ηλεκτρονικές σφραγίδες ή ηλεκτρονικές χρονοσφραγίδες για τη δημιουργία, την υπογραφή, τη σφράγιση ή τη βεβαίωση της ημερομηνίας και της ώρας, για παράδειγμα, αρχειοθέτησης αποδεικτικών στοιχείων, αρχείων αποδεικτικών στοιχείων, αρχείων συμβάντων, αρχείων ορθής εφαρμογής διαδικασιών ή εκθέσεων επιβεβαίωσης αρχειοθέτησης, θα πρέπει να χρησιμοποιούνται εγκεκριμένες υπηρεσίες εμπιστοσύνης.

(4) Το τεκμήριο συμμόρφωσης που προβλέπεται στο άρθρο 45ι παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 θα πρέπει να εφαρμόζεται μόνον όταν οι εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης συμμορφώνονται προς τις απαιτήσεις του παρόντος κανονισμού. Τα πρότυπα αναφοράς για τις εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης θα πρέπει να αποτυπώνουν καθιερωμένες πρακτικές και να χαίρουν ευρείας αναγνώρισης στους σχετικούς τομείς. Θα πρέπει να προσαρμοστούν ώστε να περιλάβουν πρόσθετους ελέγχους που κατοχυρώνουν την ασφάλεια και την αξιοπιστία των εγκεκριμένων υπηρεσιών ηλεκτρονικής αρχειοθέτησης.

(5) Εάν ένας πάροχος υπηρεσιών εμπιστοσύνης συμμορφώνεται με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό, οι εποπτικοί φορείς θα πρέπει να τεκμαίρουν τη συμμόρφωση με τις σχετικές απαιτήσεις του κανονισμού (ΕΕ) αριθ. 910/2014 και να λαμβάνουν δεόντως υπόψη το εν λόγω τεκμήριο για τη χορήγηση ή την επιβεβαίωση του καθεστώτος έγκρισης της υπηρεσίας εμπιστοσύνης. Ωστόσο, ένας εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης μπορεί ούτως ή άλλως να βασιστεί σε άλλες πρακτικές για να αποδείξει τη συμμόρφωση με τις απαιτήσεις του κανονισμού (ΕΕ) αριθ. 910/2014.

(6) Για να διαφυλάσσεται η ακεραιότητα και η απόδειξη της προέλευσης των ηλεκτρονικών δεδομένων και των ηλεκτρονικών εγγράφων που περιέχουν μία περισσότερες εγκεκριμένες ηλεκτρονικές υπογραφές ή σφραγίδες, οι εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης θα πρέπει να χρησιμοποιούν διαδικασίες και τεχνολογίες ικανές να επεκτείνουν την αξιοπιστία των εν λόγω ηλεκτρονικών υπογραφών και σφραγίδων πέραν της περιόδου τεχνολογικής ισχύος τους, τουλάχιστον καθ' όλη τη διάρκεια της περιόδου διαφύλαξης.

([1]) ΕΕ L 257 της 28.8.2014, σ. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Κανονισμός (ΕΕ) 2024/1183 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Απριλίου 2024, για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 όσον αφορά τη θέσπιση ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα (ΕΕ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(7) Η Επιτροπή αξιολογεί τακτικά νέες τεχνολογίες, πρακτικές, πρότυπα ή τεχνικές προδιαγραφές. Σύμφωνα με την αιτιολογική σκέψη 75 του κανονισμού (ΕΕ) 2024/1183, η Επιτροπή θα πρέπει να επανεξετάζει και, εάν χρειαστεί, να επικαιροποιεί τον παρόντα κανονισμό, ώστε να συμβαδίζει με τις διεθνείς εξελίξεις, τις νέες τεχνολογίες, πρακτικές, πρότυπα ή τεχνικές προδιαγραφές και να ακολουθεί τις βέλτιστες πρακτικές στην εσωτερική αγορά.

(8) Στις δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του παρόντος κανονισμού εφαρμόζεται ο κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]) και, κατά περίπτωση, η οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]).

(9) Σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]), ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις 21 Οκτωβρίου 2025 ([6]).

(10) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 48 του κανονισμού (ΕΕ) αριθ. 910/2014,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Η ηλεκτρονική αρχειοθέτηση εγγράφων που φέρουν εγκεκριμένη ηλεκτρονική υπογραφή ή εγκεκριμένη ηλεκτρονική σφραγίδα

1. Κατά την αρχειοθέτηση ηλεκτρονικών δεδομένων ή ηλεκτρονικών εγγράφων που περιέχουν εγκεκριμένες ηλεκτρονικές υπογραφές ή εγκεκριμένες ηλεκτρονικές σφραγίδες, οι πάροχοι εγκεκριμένων υπηρεσιών ηλεκτρονικής αρχειοθέτησης διασφαλίζουν ότι διαφυλάσσεται η αξιοπιστία των εν λόγω εγκεκριμένων ηλεκτρονικών υπογραφών ή εγκεκριμένων ηλεκτρονικών σφραγίδων, μεταξύ άλλων και πέραν της περιόδου τεχνολογικής ισχύος τους, και ότι διαφυλάσσεται η ακεραιότητα και η ακρίβεια της προέλευσης των εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων, τουλάχιστον έως το τέλος της περιόδου νόμιμης ή συμβατικής διαφύλαξης.

2. Για τους σκοπούς της παραγράφου 1, οι πάροχοι εγκεκριμένων υπηρεσιών ηλεκτρονικής αρχειοθέτησης μπορούν να βασίζονται σε εγκεκριμένη υπηρεσία διαφύλαξης εγκεκριμένων ηλεκτρονικών υπογραφών ή σε εγκεκριμένη υπηρεσία διαφύλαξης εγκεκριμένων ηλεκτρονικών σφραγίδων.

Άρθρο 2

Πρότυπα αναφοράς και προδιαγραφές για την παροχή εγκεκριμένων υπηρεσιών ηλεκτρονικής αρχειοθέτησης

Τα πρότυπα αναφοράς και οι προδιαγραφές που αναφέρονται στο άρθρο 45ι παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 καθορίζονται στο παράρτημα του παρόντος κανονισμού.

([3]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39, ELI: http://data. europa.eu/eli/reg/2018/1725/oj).

([6]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic archiving services. [Επίσημες παρατηρήσεις του ΕΕΠΔ επί του προσχεδίου του εκτελεστικού κανονισμού για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 όσον αφορά τα πρότυπα αναφοράς και τις προδιαγραφές για τις εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης].

Άρθρο 3

Έναρξη ισχύος

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

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

Βρυξέλλες, 16 Δεκεμβρίου 2025.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

ΠΑΡΑΡΤΗΜΑ

Κατάλογος προτύπων αναφοράς και προδιαγραφών για εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης

Ισχύει το πρότυπο CEN/TS 18170:2025 («CEN/TS 18170») με τις ακόλουθες προσαρμογές:

α) Κανονιστικές παραπομπές (σημείο 2)

— ETSI EN 319 401 V3.1.1 (2024-06) «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Απαιτήσεις γενικής πολιτικής για παρόχους υπηρεσιών εμπιστοσύνης

— ETSI EN 319 421 V1.3.1 (2025-07), Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν χρονοσφραγίδες

— ISO 14721:2025, Space Data System Practices — Reference model for an open archival information system (OAIS) [Πρακτικές του συστήματος διαστημικών δεδομένων — Μοντέλο αναφοράς για ένα ανοικτό σύστημα πληροφοριών αρχειοθέτησης (OAIS)]

— ACM-ECCG, Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, υποομάδα για την κρυπτογραφία: «Συμφωνημένοι κρυπτογραφικοί μηχανισμοί», που έχει δημοσιευτεί από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (στο εξής: ENISA).

— CIR (EU) 2024/482, εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής ([1]).

— CIR (EU) 2024/3144, εκτελεστικός κανονισμός (ΕΕ) 2024/3144 της Επιτροπής ([2]).

— ISO/IEC 15408:2022 (μέρη 1 έως 5) «Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικότητας – Κριτήρια αξιολόγησης για την ασφάλεια της τεχνολογίας πληροφοριών».

— FIPS PUB 140-3 (2019) «Απαιτήσεις ασφάλειας για κρυπτογραφικά δομοστοιχεία».

β) Δήλωση πολιτικής και πρακτικής (σημείο 6.1)

— Ισχύουν οι απαιτήσεις του CEN/TS 18170 σημείο 6.1.

— Ισχύουν οι απαιτήσεις του ETSI EN 319 401 σημείο 5.

— Ο EATSP θεσπίζει διαδικασίες για την κοινοποίηση στο εποπτικό όργανο τυχόν αλλαγών στην παροχή της υπηρεσίας εμπιστοσύνης ηλεκτρονικής αρχειοθέτησης και στην πρόθεση παύσης των εν λόγω δραστηριοτήτων, σύμφωνα με τις επιχειρηματικές απαιτήσεις και τις σχετικές νομοθετικές και κανονιστικές διατάξεις, μεταξύ άλλων σύμφωνα με τις απαιτήσεις των εκτελεστικών πράξεων που εκδίδονται δυνάμει του άρθρου 24 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.2].

— Ο EATSP κοινοποιεί στο αρμόδιο εποπτικό όργανο τουλάχιστον:

— ένα μήνα πριν από την εφαρμογή οποιασδήποτε αλλαγής·

— τρεις μήνες πριν από τη σχεδιαζόμενη παύση παροχής μιας υπηρεσίας εμπιστοσύνης.

γ) Όροι και προϋποθέσεις (σημείο 6.2)

— Ισχύουν οι απαιτήσεις του CEN/TS 18170 σημείο 6.2.

— Οι συνδρομητές και τα μέρη που βασίζονται στην υπηρεσία εμπιστοσύνης ηλεκτρονικής αρχειοθέτησης ενημερώνονται με σαφή, ολοκληρωμένο και εύκολα προσβάσιμο τρόπο, σε δημόσια προσβάσιμο χώρο και ατομικά, για τους ακριβείς όρους και τις ακριβείς προϋποθέσεις, πριν συνάψουν συμβατική σχέση.

([1]) 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).

([2]) Εκτελεστικός κανονισμός (ΕΕ) 2024/3144 της Επιτροπής, 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 (ΕΕ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

δ) Ανθρώπινοι πόροι (σημείο 7.3)

— Ισχύουν οι απαιτήσεις του CEN/TS 18170 σημείο 7.3.

— Τα μέλη του προσωπικού του EATSP που έχουν αναλάβει ρόλους εμπιστοσύνης και, κατά περίπτωση, οι υπεργολάβοι τους που έχουν αναλάβει ρόλους εμπιστοσύνης, είναι σε θέση να πληρούν την απαίτηση για «εξειδικευμένες γνώσεις, πείρα και προσόντα» μέσω τυπικής κατάρτισης και διαπιστευτηρίων, ή πραγματικής πείρας, ή συνδυασμού των δύο. Εν προκειμένω περιλαμβάνονται τακτικές ενημερώσεις (τουλάχιστον κάθε 12 μήνες) σχετικά με τις νέες απειλές και τις τρέχουσες πρακτικές ασφάλειας.

ε) Κρυπτογραφικοί έλεγχοι και παρακολούθηση (σημείο 7.6)

— Το σύστημα αρχειοθέτησης πρέπει να εγγυάται την εμπιστευτικότητα των δεδομένων και των εγγράφων καθ' όλη τη διάρκεια του κύκλου ζωής του αρχείου, από την κατάθεσή του έως την κατάργησή του.

— Ισχύουν οι απαιτήσεις που καθορίζονται στο ETSI EN 319 401 υποσημείο 7.5 «Κρυπτογραφικοί έλεγχοι».

— Η προέλευση των δεδομένων που προορίζονται προς αρχειοθέτηση στο σύστημα ηλεκτρονικής αρχειοθέτησης καθορίζεται από τον EATSP. Εάν για τον σκοπό αυτόν χρησιμοποιούν ηλεκτρονικές υπογραφές ή ηλεκτρονικές σφραγίδες, οι εν λόγω ηλεκτρονικές υπογραφές ή ηλεκτρονικές σφραγίδες είναι εγκεκριμένες.

— Όταν ο EATSP υπογράφει ψηφιακά ψηφιακό αντικείμενο ή εγγραφή (ή μέρος τους), το ιδιωτικό κλειδί υπογραφής του EATSP διατηρείται και χρησιμοποιείται είτε σε διάταξη δημιουργίας εγκεκριμένης ηλεκτρονικής υπογραφής ή σφραγίδας είτε σε ασφαλή κρυπτογραφική διάταξη που αποτελεί αξιόπιστο σύστημα πιστοποιημένο σύμφωνα με:

  α) κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας των πληροφοριών, τα οποία καθορίζονται στο ISO/IEC 15408 ή στα κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας των πληροφοριών, έκδοση CC:2022, Μέρη 1 έως 5, που δημοσιεύτηκαν από τους συμμετέχοντες στη ρύθμιση για την αναγνώριση των πιστοποιητικών κοινών κριτηρίων στον τομέα της ασφάλειας της ΤΠ, και πιστοποιημένα κατά το πρότυπο EAL 4 ή ανώτερο· ή

  β) το ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων [CIR (EU) 2024/482, CIR (EU) 2024/3144], και πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

  γ) έως τις 31.12.2030, το FIPS PUB 140-3 επίπεδο 3.

— Η πιστοποίηση αυτή αφορά στόχο ασφάλειας ή προφίλ προστασίας, ή σχεδιασμό δομοστοιχείου και τεκμηρίωση ασφάλειας, που πληροί τις απαιτήσεις του παρόντος εγγράφου, βάσει ανάλυσης κινδύνου και λαμβανομένων υπόψη φυσικών και άλλων μη τεχνικών μέτρων ασφάλειας.

— Εάν η ασφαλής κρυπτογραφική διάταξη διαθέτει πιστοποίηση EUCC [IR (EU) 2024/482, CIR (EU) 2024/3144], τότε η διάταξη αυτή διαμορφώνεται και χρησιμοποιείται σύμφωνα με την εν λόγω πιστοποίηση.

— Ο EATSP παρακολουθεί την ισχύ του κρυπτογραφικού αλγορίθμου που χρησιμοποιήθηκε και χρησιμοποιείται. Σε περίπτωση που ένας από τους χρησιμοποιούμενους αλγόριθμους ή τις χρησιμοποιούμενες παραμέτρους θεωρείται ότι δεν είναι κατάλληλος ή κατάλληλη, όπως ορίζεται στη διαχείριση κινδύνου, ο EATSP είτε επικαιροποιεί τη σχετική πολιτική αρχειοθέτησης είτε δημιουργεί νέο προφίλ αρχειοθέτησης για τον χειρισμό των AIP και εκπονεί και εφαρμόζει κατάλληλα μέτρα.

— Η αξιολόγηση των κρυπτογραφικών αλγορίθμων και της χρήσης τους από τον EATSP συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA (ACM-ECCG).

— Τα τεχνικά στοιχεία των EATS επαληθεύουν αμοιβαία την ταυτότητά τους βάσει τεχνικών κρυπτογράφησης πριν επικοινωνήσουν.

στ) Δίκτυο (σημείο 7.9)

— Ισχύουν οι απαιτήσεις που καθορίζονται στο ETSI EN 319 401 υποσημείο 7.8 «Ασφάλεια δικτύου».

— Η σάρωση τρωτών σημείων που απαιτείται από το REQ-7.8-13 του ETSI EN 319 401 εκτελείται τουλάχιστον μία φορά ανά τρίμηνο.

— Η δοκιμή παρείσδυσης που απαιτείται από τη REQ-7.8-17X του ETSI EN 319 401 εκτελείται τουλάχιστον μία φορά ετησίως.

— Τα τείχη προστασίας διαμορφώνονται έτσι ώστε να αποτρέπονται όλα τα πρωτόκολλα και οι προσβάσεις που δεν απαιτούνται για τη λειτουργία του EATSP.

ζ) Συλλογή αποδεικτικών στοιχείων (σημείο 7.11)

— Ισχύουν οι απαιτήσεις που καθορίζονται στο ETSI EN 319 401 υποσημείο 7.10 «Συλλογή αποδεικτικών στοιχείων», μεταξύ άλλων και για κρίσιμα και μη κρίσιμα συμβάντα (βλέπε υποσημείο 13.2)

η) Τερματισμός και σχέδιο τερματισμού ενός EATSP (σημείο 7.13)

— Ισχύουν οι απαιτήσεις του CEN/TS 18170 σημείο 7.13.

— Το σχέδιο τερματισμού του EATSP συμμορφώνεται με τις απαιτήσεις που ορίζονται στις εκτελεστικές πράξεις που εκδίδονται σύμφωνα με το άρθρο 24 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 910/2014.

θ) Αξιόπιστος χρόνος συμβάντων (σημείο 13.3.1)

— Ισχύουν οι απαιτήσεις του CEN/TS 18170 σημείο 13.3.1.

— Κατά τη χρήση χρονοσφραγίδων, ο EATSP χρησιμοποιεί εγκεκριμένη χρονοσφραγίδα.