Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/2531

17.12.2025

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/2531 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 τα εγκεκριμένα ηλεκτρονικά καθολικά

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 45ιβ παράγραφος 3,

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 καταγραφής ηλεκτρονικών δεδομένων σε εγκεκριμένο ηλεκτρονικό καθολικό. Η Επιτροπή καλείται να καταρτίσει κατάλογο προτύπων αναφοράς και, όπου είναι απαραίτητο, να θεσπίσει προδιαγραφές για αυτές τις υπηρεσίες.

(2) Ένα ηλεκτρονικό καθολικό είναι μια ακολουθία ηλεκτρονικών εγγραφών δεδομένων, η οποία διασφαλίζει την ακεραιότητα των εν λόγω εγγραφών δεδομένων και την ακρίβεια της χρονολογικής σειράς των εν λόγω εγγραφών. Προκειμένου να διασφαλιστεί ότι η καταχώριση δεδομένων σε εγκεκριμένο ηλεκτρονικό καθολικό είναι χρονολογικά διατεταγμένη, συνεπής και αξιόπιστη, είναι αναγκαίο να θεσπιστεί ένα κοινό σύνολο προδιαγραφών για την καταγραφή ηλεκτρονικών δεδομένων σε εγκεκριμένο ηλεκτρονικό καθολικό.

(3) Το τεκμήριο συμμόρφωσης που προβλέπεται στο άρθρο 45ιβ παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 θα πρέπει να εφαρμόζεται μόνον όταν οι εγκεκριμένες υπηρεσίες εμπιστοσύνης για την καταγραφή ηλεκτρονικών δεδομένων σε εγκεκριμένο ηλεκτρονικό καθολικό συμμορφώνονται με τα πρότυπα που ορίζονται στον παρόντα κανονισμό. Τα πρότυπα αυτά 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 εμπιστοσύνης.

(4) Εάν ένας πάροχος υπηρεσιών εμπιστοσύνης συμμορφώνεται με τις απαιτήσεις που ορίζονται στο παράρτημα του παρόντος κανονισμού, 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.

(5) 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 χρειάζεται, 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.

([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).

(6) Στις δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού εφαρμόζονται 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]), λαμβάνοντας επίσης υπόψη τις «Κατευθυντήριες γραμμές 02/2025 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω τεχνολογιών αλυσίδας συστοιχιών» ([5]).

(7) Σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([6]), ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις 21 Οκτωβρίου 2025 ([7]).

(8) 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

Πρότυπα αναφοράς και προδιαγραφές

Τα πρότυπα αναφοράς και οι προδιαγραφές που αναφέρονται στο άρθρο 45ιβ παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 910/2014 καθορίζονται, για τα εγκεκριμένα ηλεκτρονικά καθολικά, στο παράρτημα του παρόντος κανονισμού.

Άρθρο 2

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

([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]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 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).

([7]) 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 ledgers (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 τα εγκεκριμένα ηλεκτρονικά καθολικά).

ΠΑΡΑΡΤΗΜΑ

Κατάλογος τεχνικών προδιαγραφών και προτύπων αναφοράς για εγκεκριμένα κατανεμημένα ηλεκτρονικά καθολικά

1. Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

   α) «οριστικότητα»: η κατάσταση μιας εγγραφής δεδομένων ηλεκτρονικού καθολικού στην οποία η εγγραφή έχει καταστεί μη αναστρέψιμη και δεν μπορεί να τροποποιηθεί ή να αφαιρεθεί·

   β) «κατανεμημένο ηλεκτρονικό καθολικό»: ηλεκτρονικό καθολικό που μοιράζεται σε σύνολο κόμβων κατανεμημένου ηλεκτρονικού καθολικού και συγχρονίζεται μεταξύ των κόμβων του κατανεμημένου ηλεκτρονικού καθολικού με τη χρήση μηχανισμού συναίνεσης·

   γ) «κόμβος κατανεμημένου ηλεκτρονικού καθολικού»: διάταξη ή διαδικασία που αποτελεί μέρος δικτύου κατανεμημένου ηλεκτρονικού καθολικού και αποθηκεύει πλήρες ή μερικό αντίγραφο των καταγραφών δεδομένων ενός ηλεκτρονικού καθολικού·

   δ) «δίκτυο κατανεμημένου ηλεκτρονικού καθολικού»: δίκτυο κόμβων κατανεμημένου ηλεκτρονικού καθολικού που αποτελεί σύστημα κατανεμημένου ηλεκτρονικού καθολικού·

   ε) «σύστημα κατανεμημένου ηλεκτρονικού καθολικού»: σύστημα που υλοποιεί κατανεμημένο ηλεκτρονικό καθολικό·

   στ) «συναίνεση»: συμφωνία μεταξύ κόμβων κατανεμημένου ηλεκτρονικού καθολικού σχετικά με την εγκυρότητα των συναλλαγών και τη διατήρηση συνεκτικού και διατεταγμένου συνόλου επικυρωμένων συναλλαγών σε ολόκληρο το σύστημα του κατανεμημένου ηλεκτρονικού καθολικού·

   ζ) «μηχανισμός συναίνεσης»: το σύνολο κανόνων και διαδικασιών με το οποίο επιτυγχάνεται συναίνεση·

   η) «εφαρμοστέοι κανόνες»: το σύνολο πρωτοκόλλων, πολιτικών και μηχανισμών που υπαγορεύει τον τρόπο λειτουργίας του συστήματος του κατανεμημένου ηλεκτρονικού καθολικού, τον τρόπο επικύρωσης και προσθήκης δεδομένων σε ένα ηλεκτρονικό καθολικό και τον τρόπο αλληλεπίδρασης των συμμετεχόντων·

   θ) «συναλλαγή»: η μικρότερη δυνατή μονάδα μιας διεργασίας εργασίας εντός ενός ηλεκτρονικού καθολικού·

   ι) «διεργασία εργασίας»: μία ή περισσότερες ακολουθίες ενεργειών που απαιτούνται για την παραγωγή αποτελέσματος το οποίο συμμορφώνεται με τους κανόνες λειτουργίας ενός ηλεκτρονικού καθολικού·

   ια) «επικυρωμένη συναλλαγή»: συναλλαγή της οποίας οι απαιτούμενοι όροι που σχετίζονται με την ακεραιότητα, τη γνησιότητα και το πρωτόκολλο έχουν ελεγχθεί σύμφωνα με τους εφαρμοστέους κανόνες του συστήματος του κατανεμημένου ηλεκτρονικού καθολικού·

   ιβ) «κρυπτογραφικός σύνδεσμος»: αναφορά σε δεδομένα που δημιουργείται με τη χρήση κατάλληλων κρυπτογραφικών τεχνικών για τη διασφάλιση της ακεραιότητας, της γνησιότητας ή της ιχνηλασιμότητας των δεδομένων στα οποία γίνεται η αναφορά και της ορθής αλληλουχίας των εγγραφών δεδομένων·

   ιγ) «έκθεση καθολικού»: δομημένη παρουσίαση επαληθεύσιμων πληροφοριών που εξάγονται από τις εγγραφές δεδομένων ενός ηλεκτρονικού καθολικού, η οποία παρέχει πληροφορίες σχετικά με συγκεκριμένες δραστηριότητες, καταστάσεις ή συμμόρφωση με προκαθορισμένους κανόνες·

   ιδ) «πάροχος εγκεκριμένου ηλεκτρονικού καθολικού»: πάροχος εγκεκριμένων υπηρεσιών εμπιστοσύνης που παρέχει εγκεκριμένη υπηρεσία εμπιστοσύνης η οποία συνίσταται στην καταχώριση δεδομένων σε εγκεκριμένο ηλεκτρονικό καθολικό.

   ιε) «εγκεκριμένο κατανεμημένο ηλεκτρονικό καθολικό»: κατανεμημένο ηλεκτρονικό καθολικό που πληροί τις απαιτήσεις για ένα εγκεκριμένο ηλεκτρονικό καθολικό.

2. Όταν ο πάροχος εγκεκριμένων υπηρεσιών εμπιστοσύνης πρέπει να συντάξει έκθεση καθολικού, αυτή συντάσσεται με αυτοματοποιημένο τρόπο.

3. Οι πάροχοι εγκεκριμένων ηλεκτρονικών καθολικών δημιουργούν εγκεκριμένο ηλεκτρονικό καθολικό, καταγράφουν ηλεκτρονικά δεδομένα σε αυτό, το επικαιροποιούν και το διατηρούν σύμφωνα με τις προδιαγραφές που καθορίζονται:

   α) Για όλους τους παρόχους εγκεκριμένων ηλεκτρονικών καθολικών, στο ETSI EN 319 401 v3.1.1 (2024-06) με τις ακόλουθες προσαρμογές:

      — 2.1 Κανονιστικές παραπομπές:

      [1] Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, υποομάδα για την κρυπτογραφία: «Συμφωνημένοι κρυπτογραφικοί μηχανισμοί» που δημοσιεύτηκε από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (στο εξής: ENISA).

[2] IETF RFC 7515 (Μάιος 2015): «JSON Web Signature (JWS)».

[3] FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules».

[4] 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 (στο εξής: EUCC).

[5] 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.

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

— 6.1 Δήλωση πρακτικών υπηρεσιών εμπιστοσύνης:

  — REQ-6.1-12 Η δήλωση πρακτικής ενός ηλεκτρονικού καθολικού περιλαμβάνει τουλάχιστον τις ακόλουθες πληροφορίες:

    — τις λειτουργικές και τεχνικές ικανότητες της πλατφόρμας ηλεκτρονικού καθολικού και τη χρήση της κατά την παροχή της καταγραφής δεδομένων σε εγκεκριμένο ηλεκτρονικό καθολικό ως εγκεκριμένη υπηρεσία εμπιστοσύνης·

    — τους συγκεκριμένους μηχανισμούς επαλήθευσης της προέλευσης των δεδομένων που χρησιμοποιούνται κατά την παροχή της υπηρεσίας·

    — τους συγκεκριμένους μηχανισμούς ακολουθιακής χρονολογικής παραγγελίας που χρησιμοποιούνται κατά την παροχή της υπηρεσίας.

    — κατά περίπτωση, την κρυπτογραφική ζεύξη που χρησιμοποιείται για τη διασφάλιση της αλληλουχίας των εγγραφών δεδομένων·

    — κατά περίπτωση, τον μηχανισμό συναίνεσης που διασφαλίζει την οριστικότητα και την ακεραιότητα των εγγραφών δεδομένων και των συναλλαγών που αποθηκεύονται στο καθολικό, συμπεριλαμβανομένου τυχόν χρόνου προφύλαξης έως ότου επέλθει η οριστικότητα και η ακεραιότητα·

    — τους ειδικούς μηχανισμούς ακεραιότητας των δεδομένων που χρησιμοποιούνται κατά την παροχή της υπηρεσίας.

  — 6.2 Όροι και προϋποθέσεις:

    — REQ-6.2-03 Οι συνδρομητές και τα μέρη που βασίζονται στην υπηρεσία εμπιστοσύνης ενημερώνονται με σαφή, ολοκληρωμένο και εύκολα προσβάσιμο τρόπο, σε δημόσια προσβάσιμο χώρο και ατομικά, για τους ακριβείς όρους και τις ακριβείς προϋποθέσεις, συμπεριλαμβανομένων των στοιχείων που απαριθμούνται ανωτέρω, πριν συνάψουν συμβατική σχέση.

  — 6.3 Πολιτική ασφάλειας πληροφοριών:

    — REQ-6.3-04X Η TSP θεσπίζει διαδικασίες για την κοινοποίηση στο εποπτικό όργανο τυχόν αλλαγών σχετικά με την παροχή της υπηρεσίας εμπιστοσύνης, σύμφωνα με τις επιχειρηματικές απαιτήσεις και τις σχετικές νομοθετικές και κανονιστικές διατάξεις. Η TSP ενημερώνει το εποπτικό όργανο τουλάχιστον:

      — ένα μήνα πριν από την εφαρμογή οποιασδήποτε αλλαγής·

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

  — 7.2 Ανθρώπινοι πόροι:

    — REQ-7.2-04X Τα μέλη του προσωπικού της TSP που έχουν ρόλο εμπιστοσύνης πληρούν την απαίτηση για «εξειδικευμένες γνώσεις, πείρα και προσόντα» μέσω τυπικής κατάρτισης και διαπιστευτηρίων, ή πραγματικής πείρας, ή συνδυασμού των δύο.

— REQ-7.2-05X Το στοιχείο αυτό περιλαμβάνει τακτικές (τουλάχιστον ανά 12 μήνες) ενημερώσεις σχετικά με τις νέες απειλές και τις τρέχουσες πρακτικές ασφάλειας.

— 7.5 Κρυπτογραφικοί έλεγχοι:

— REQ-7.5-01X Εφαρμόζονται κατάλληλοι έλεγχοι ασφάλειας για τη διαχείριση τυχόν κρυπτογραφικών κλειδιών, κρυπτογραφικών αλγορίθμων και κρυπτογραφικών συσκευών καθ' όλη τη διάρκεια του κύκλου ζωής τους, ακολουθώντας, κατά περίπτωση, προσέγγιση κρυπτογραφικής ευελιξίας.

— REQ-7.5-02 Για τους σκοπούς της παροχής των υπηρεσιών εμπιστοσύνης της, η TSP επιλέγει και χρησιμοποιεί κατάλληλες κρυπτογραφικές τεχνικές σύμφωνες με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που έχει εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και έχει δημοσιεύσει ο ENISA [1].

Ειδικότερα:

— REQ-7.5-03 Οι πάροχοι εγκεκριμένων ηλεκτρονικών καθολικών καθορίζουν την προέλευση των εγγραφών δεδομένων στο ηλεκτρονικό καθολικό. Στο πλαίσιο αυτό, χρησιμοποιούν προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε εγκεκριμένα πιστοποιητικά ή προηγμένες ηλεκτρονικές σφραγίδες βάσει εγκεκριμένων πιστοποιητικών δημιουργημένων από τους χρήστες της υπηρεσίας σύμφωνα με τα ακόλουθα πρότυπα και προδιαγραφές:

α) ETSI EN 319 122-1 V1.3.1 (2023-06). Electronic Signatures and Infrastructures (ESI) [Ηλεκτρονικές υπογραφές και υποδομές (ESI)]· ψηφιακές υπογραφές CAdES· Μέρος 1: δομικά στοιχεία και βασικές υπογραφές CAdES.

β) ETSI EN 319 132-1 V1.3.1 (2024-07). Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· ψηφιακές υπογραφές XAdES· Μέρος 1: δομικά στοιχεία και βασικές υπογραφές XAdES.

γ) ETSI TS 119 182-1 V1.2.1 (2024-07). Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· ψηφιακές υπογραφές JAdES· Μέρος 1: δομικά στοιχεία και βασικές υπογραφές JAdES, με την ακόλουθη προσαρμογή:

— 5.1.8 Η παράμετρος κεφαλίδας x5c (Αλυσίδα πιστοποιητικών X.509)

— Η παράμετρος κεφαλίδας x5c, όπως ορίζεται στο σημείο 4.1.6 του IETF RFC 7515 [2], περιλαμβάνεται στην υπογραφή JAdES, είτε ως υπογεγραμμένη είτε ως μη υπογεγραμμένη παράμετρος κεφαλίδας.

— Η παράμετρος κεφαλίδας x5c έχει τη σημασιολογία που καθορίζεται στο σημείο 4.1.6 του IETF RFC 7515 [2].

— Η παράμετρος κεφαλίδας x5c έχει τη σύνταξη που καθορίζεται στο IETF RFC 7515 [2] σημείο 4.1.6.

— REQ-7.5-04: Οι πάροχοι εγκεκριμένων ηλεκτρονικών καθολικών διασφαλίζουν τη μοναδική ακολουθιακή χρονολογική διάταξη των εγγραφών δεδομένων στο ηλεκτρονικό καθολικό. Στο πλαίσιο αυτό, χρησιμοποιούν κρυπτογραφικούς συνδέσμους που βασίζονται σε λίστες κατακερματισμού ή δέντρα κατακερματισμού, χρησιμοποιώντας κρυπτογραφικές συναρτήσεις κατακερματισμού, σύμφωνα με τις ακόλουθες προδιαγραφές και τα ακόλουθα πρότυπα:

α) SHA-256 ή μεγαλύτερο μέγεθος κατακερματισμού στην εκροή σύμφωνα με τους «συμφωνημένους κρυπτογραφικούς μηχανισμούς» που έχει εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και έχει δημοσιεύσει ο ENISA [1].

β) SHA3-256 ή μεγαλύτερο μέγεθος κατακερματισμού στην εκροή σύμφωνα με τους «συμφωνημένους κρυπτογραφικούς μηχανισμούς» που έχει εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και έχει δημοσιεύσει ο ENISA [1].

Εναλλακτικά, κατά τη χρήση της καταγραφής της χρονικής στιγμής για τη διασφάλιση της μοναδικής ακολουθιακής χρονολογικής διάταξης των εγγραφών δεδομένων στο ηλεκτρονικό καθολικό, οι πάροχοι εγκεκριμένων ηλεκτρονικών καθολικών χρησιμοποιούν εγκεκριμένες χρονοσφραγίδες.

— REQ-7.5-05 Οι πάροχοι εγκεκριμένων ηλεκτρονικών καθολικών διασφαλίζουν την ακεραιότητα των εγγραφών δεδομένων που καταγράφονται σε εγκεκριμένο ηλεκτρονικό καθολικό. Στο πλαίσιο αυτό, χρησιμοποιούν προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε εγκεκριμένα πιστοποιητικά ή προηγμένες ηλεκτρονικές σφραγίδες που βασίζονται σε εγκεκριμένα πιστοποιητικά, σύμφωνα με τα ακόλουθα πρότυπα και τις ακόλουθες προδιαγραφές:

    α) κάθε μορφότυπος υπογραφής ή σφραγίδας που συμμορφώνεται με τους «συμφωνημένους κρυπτογραφικούς μηχανισμούς» που έχει εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και έχει δημοσιεύσει ο ENISA [1]·

    β) SHA-256 ή μεγαλύτερο μέγεθος κατακερματισμού στην εκροή σύμφωνα με τους «συμφωνημένους κρυπτογραφικούς μηχανισμούς» που έχει εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και έχει δημοσιεύσει ο ENISA [1]·

    γ) SHA3-256 ή μεγαλύτερο μέγεθος κατακερματισμού στην εκροή σύμφωνα με τους «συμφωνημένους κρυπτογραφικούς μηχανισμούς» που έχει εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και έχει δημοσιεύσει ο ENISA [1].

    δ) Οι πάροχοι εγκεκριμένων ηλεκτρονικών καθολικών διασφαλίζουν την άμεση ανιχνευσιμότητα κάθε μεταγενέστερης αλλαγής στα δεδομένα που καταγράφονται σε εγκεκριμένο ηλεκτρονικό καθολικό.

— REQ-7.5-06 Στις περιπτώσεις στις οποίες χρησιμοποιούνται μηχανισμοί ψηφιακής υπογραφής, τα ιδιωτικά κλειδιά υπογραφής του παρόχου του εγκεκριμένου ηλεκτρονικού καθολικού διατηρούνται και χρησιμοποιούνται εντός ασφαλούς κρυπτογραφικής διάταξης που συνιστά αξιόπιστο σύστημα πιστοποιημένο σύμφωνα με:

    α) κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας των πληροφοριών, τα οποία καθορίζονται στο ISO/IEC 15408 ([1]) [6] ή στα κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας των 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 της ΤΠ, και πιστοποιημένα κατά το πρότυπο EAL 4 ή ανώτερο· or

    β) το ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (EUCC) ([2]) ([3]) [4][5], και πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· or

    γ) έως τις 31.12.2030, το FIPS PUB 140-3 ([4]) [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 [4][5], τότε η διάταξη αυτή διαμορφώνεται και χρησιμοποιείται σύμφωνα με την εν λόγω πιστοποίηση.

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

([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/2024/482/2025-01-08).

([3]) 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).

([4]) FIPS PUB 140-3 (2019): «Απαιτήσεις ασφάλειας για κρυπτογραφικά δομοστοιχεία».

— 7.8 Ασφάλεια δικτύου:

— REQ-7.8-14X Η σάρωση τρωτών σημείων που απαιτείται από τη REQ-7.8-13 εκτελείται τουλάχιστον μία φορά ανά τρίμηνο.

— REQ-7.8-18X Η δοκιμή παρείσδυσης που απαιτείται από τη REQ-7.8-17X εκτελείται τουλάχιστον μία φορά ετησίως.

— REQ-7.8-21X: Τα τείχη προστασίας διαμορφώνονται επίσης έτσι ώστε να αποτρέπονται όλα τα πρωτόκολλα και οι προσβάσεις που δεν απαιτούνται για τη λειτουργία του παρόχου υπηρεσιών εμπιστοσύνης.

— 7.9.1 Παρακολούθηση και τήρηση μητρώου:

— REQ-7.9.1-02X Οι δραστηριότητες παρακολούθησης λαμβάνουν υπόψη τον ευαίσθητο χαρακτήρα των πληροφοριών που συλλέγονται ή αναλύονται.

— 7.12 Τερματισμός και σχέδια τερματισμού του παρόχου υπηρεσιών εμπιστοσύνης:

— REQ-7.12-02A Το σχέδιο τερματισμού του παρόχου υπηρεσιών εμπιστοσύνης συμμορφώνεται με τις απαιτήσεις που ορίζονται στις εκτελεστικές πράξεις που εκδίδονται σύμφωνα με το άρθρο 24 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1].

β) Επιπλέον, για όλους τους παρόχους εγκεκριμένων ηλεκτρονικών καθολικών που χρησιμοποιούν τεχνολογίες κατανεμημένου ηλεκτρονικού καθολικού:

1) ISO 23257:2022 Τεχνολογίες αλυσίδας συστοιχιών και κατανεμημένου καθολικού — αρχιτεκτονική αναφοράς, σημείο 9, το οποίο παρέχει πλήρη περιγραφή του συστήματος τεχνολογίας κατανεμημένου ηλεκτρονικού καθολικού, του αντίστοιχου δικτύου τεχνολογίας κατανεμημένου ηλεκτρονικού καθολικού και των κόμβων τεχνολογίας κατανεμημένου ηλεκτρονικού καθολικού·

2) ISO/TS 23635:2022 Τεχνολογίες αλυσίδας συστοιχιών και κατανεμημένου καθολικού — Κατευθυντήριες γραμμές για τη διακυβέρνηση, όσον αφορά τις γραπτές και δημοσίως προσβάσιμες πολιτικές και πρακτικές που σχετίζονται με τη δομή διακυβέρνησης για την υπηρεσία ηλεκτρονικού καθολικού που παρέχουν.