Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/1946

30.9.2025

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/1946 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 29ης Σεπτεμβρίου 2025

για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τις εγκεκριμένες υπηρεσίες διαφύλαξης εγκεκριμένων ηλεκτρονικών υπογραφών και εγκεκριμένων ηλεκτρονικών σφραγίδων

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 34 παράγραφος 2 και το άρθρο 40,

Εκτιμώντας τα ακόλουθα:

(1) Οι εγκεκριμένες υπηρεσίες διαφύλαξης εγκεκριμένων ηλεκτρονικών υπογραφών και εγκεκριμένων ηλεκτρονικών σφραγίδων διασφαλίζουν τη μακροπρόθεσμη ακεραιότητα, γνησιότητα, απόδειξη ύπαρξης και προσβασιμότητα των αποδεικτικών στοιχείων διαφύλαξης των εν λόγω ηλεκτρονικών υπογραφών και ηλεκτρονικών σφραγίδων. Αυτό καθιστά δυνατή την απόδειξη της νομικής τους ισχύος για παρατεταμένες χρονικές περιόδους και εγγυάται τη δυνατότητα επικύρωσής τους ανεξάρτητα από τις μελλοντικές τεχνολογικές αλλαγές. Οι υπηρεσίες αυτές παρέχονται ανεξάρτητα ή στο πλαίσιο άλλης εγκεκριμένης υπηρεσίας εμπιστοσύνης, όπως οι εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης.

(2) Το τεκμήριο συμμόρφωσης που προβλέπεται στο άρθρο 34 παράγραφος 1α και στο άρθρο 40 του κανονισμού (ΕΕ) αριθ. 910/2014 θα πρέπει να εφαρμόζεται μόνο όταν οι εγκεκριμένες υπηρεσίες διαφύλαξης εγκεκριμένων ηλεκτρονικών υπογραφών και εγκεκριμένων ηλεκτρονικών σφραγίδων συμμορφώνονται με τα πρότυπα που ορίζονται στον παρόντα κανονισμό. Τα πρότυπα αυτά θα πρέπει να αντικατοπτρίζουν καθιερωμένες πρακτικές και να αναγνωρίζονται ευρέως στους σχετικούς τομείς. Θα πρέπει να προσαρμοστούν ώστε να περιλαμβάνουν πρόσθετους ελέγχους που διασφαλίζουν την ασφάλεια και την αξιοπιστία της εγκεκριμένης υπηρεσίας εμπιστοσύνης, καθώς και την ικανότητα επαλήθευσης του χαρακτηρισμού των υπογραφών και των σφραγίδων ως εγκεκριμένων, αφενός, και της τεχνικής εγκυρότητάς τους με την πάροδο του χρόνου, αφετέρου.

(3) 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 χαρακτηρισμού της υπηρεσίας εμπιστοσύνης ως εγκεκριμένης. 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.

(4) Η Επιτροπή αξιολογεί τακτικά νέες τεχνολογίες, πρακτικές, πρότυπα ή τεχνικές προδιαγραφές. Σύμφωνα με την αιτιολογική σκέψη 75 του κανονισμού (ΕΕ) 2024/1183 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]), η Επιτροπή θα πρέπει να επανεξετάζει και, εάν χρειάζεται, να επικαιροποιεί τον παρόντα κανονισμό, ώστε να συμβαδίζει με τις διεθνείς εξελίξεις, τις νέες τεχνολογίες, τα πρότυπα ή τις 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).

(5) 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]).

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

(7) 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 34 παράγραφος 2 και στο άρθρο 40 του κανονισμού (ΕΕ) αριθ. 910/2014 καθορίζονται 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, 29 Σεπτεμβρίου 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]) 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).

ΠΑΡΑΡΤΗΜΑ

Κατάλογος προτύπων αναφοράς και προδιαγραφών που αναφέρονται στο άρθρο 2

Ισχύουν τα πρότυπα ETSI TS 119 511 V1.1.1 (2019-06) («ETSI TS 119 511») και ETSI TS 119 172-4 V1.1.1 (2021-05) («ETSI TS 119 172-4») με τις ακόλουθες προσαρμογές:

1. Όσον αφορά το ETSI TS 119 511

1) 2.1 Κανονιστικές παραπομπές:

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

— [2] ETSI TS 119 612 (V2.3.1) «Ηλεκτρονικές Υπογραφές και Υποδομές (ESI)· Κατάλογοι εμπιστοσύνης».

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

— [6] Εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής ([1]) 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).

— [7] Εκτελεστικός κανονισμός (ΕΕ) 2024/3144 της Επιτροπής ([2]) για την τροποποίηση του εκτελεστικού κανονισμού (ΕΕ) 2024/482 όσον αφορά τα εφαρμοστέα διεθνή πρότυπα και για τη διόρθωση του εν λόγω εκτελεστικού κανονισμού.

— [8] Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, υποομάδα για την κρυπτογραφία: «Συμφωνημένοι κρυπτογραφικοί μηχανισμοί» που δημοσιεύτηκε από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (στο εξής: ENISA) ([3]).

— [9] ETSI TS 119 172-4 V1.1.1 (2021-05) «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Πολιτικές υπογραφών: Μέρος 4: Κανόνες εφαρμογής υπογραφής (πολιτική επικύρωσης) για τις ευρωπαϊκές εγκεκριμένες ηλεκτρονικές υπογραφές/σφραγίδες με τη χρήση καταλόγων εμπιστοσύνης».

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

2) 3.1 Όροι

— ασφαλής κρυπτογραφική διάταξη: διάταξη που διατηρεί το ιδιωτικό κλειδί του χρήστη, προστατεύει το κλειδί αυτό από έκθεση σε κίνδυνο και εκτελεί λειτουργίες υπογραφής ή αποκρυπτογράφησης για λογαριασμό του χρήστη.

3) 6.4 Προφίλ διαφύλαξης

— OVR-6.4-08A [WTS][WOS] Η αναμενόμενη περίοδος διατήρησης των αποδεικτικών στοιχείων συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

— ΣΗΜΕΙΩΣΗ 3 άκυρο.

4) 6.5 Πολιτική διαφύλαξης αποδεικτικών στοιχείων

— OVR-6.5-04A Οι χρησιμοποιούμενοι αλγόριθμοι κρυπτογράφησης συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

— ΣΗΜΕΙΩΣΗ 1 άκυρο.

([1]) ΕΕ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([2]) ΕΕ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

5) 7.2 Ανθρώπινοι πόροι

— OVR-7.2-02 Τα μέλη του προσωπικού του παρόχου υπηρεσιών πληρωμών 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.

— OVR-7.2-03 Η συμμόρφωση με το OVR-7.2-02 περιλαμβάνει τακτικές ενημερώσεις (τουλάχιστον κάθε 12 μήνες) σχετικά με τις νέες απειλές και τις τρέχουσες πρακτικές ασφάλειας.

6) 7.5 Κρυπτογραφικοί έλεγχοι

— OVR-7.5-05 [ΥΠΟ ΟΡΟΥΣ] Με την υπογραφή από τον πάροχο υπηρεσιών πληρωμών (μέρους) των αποδεικτικών στοιχείων διαφύλαξης, το ιδιωτικό κλειδί υπογραφής του παρόχου υπηρεσιών πληρωμών διατηρείται και χρησιμοποιείται εντός ασφαλούς κρυπτογραφικής διάταξης που συνιστά αξιόπιστο σύστημα το οποίο είναι πιστοποιημένο σύμφωνα με:

α) κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας των πληροφοριών, τα οποία καθορίζονται στο ISO/IEC 15408 [10] 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 πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

β) EUCC [6][7] και πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

γ) έως τις 31.12.2030, το FIPS PUB 140-3 [5] 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 [6][7], τότε η διάταξη αυτή διαμορφώνεται και χρησιμοποιείται σύμφωνα με την εν λόγω πιστοποίηση.

— OVR-7.5-06 [ΥΠΟ ΟΡΟΥΣ] άκυρο.

— OVR-7.5-07 [ΥΠΟ ΟΡΟΥΣ] Με την υπογραφή από τον πάροχο υπηρεσιών πληρωμών (μέρους) των αποδεικτικών στοιχείων διαφύλαξης, τυχόν αντίγραφα ασφάλειας των ιδιωτικών κλειδιών υπογραφής του παρόχου υπηρεσιών πληρωμών προστατεύονται με την ασφαλή κρυπτογραφική διάταξη ώστε να διασφαλίζεται η ακεραιότητα και ο εμπιστευτικός χαρακτήρας τους, προτού αυτά αποθηκευτούν εκτός της εν λόγω διάταξης.

— OVR-7.5-08 Το ιδιωτικό κλειδί υπογραφής ενός παρόχου υπηρεσιών πληρωμών εξάγεται και εισάγεται σε διαφορετική ασφαλή κρυπτογραφική διάταξη μόνον όταν η εν λόγω εξαγωγή και εισαγωγή πραγματοποιούνται με ασφάλεια και σύμφωνα με την πιστοποίηση των εν λόγω διατάξεων.

7) 7.8 Ασφάλεια δικτύου

— OVR-7.8-03 Η σάρωση τρωτών σημείων που απαιτείται από το REQ-7.8-13 του ETSI EN 319 401 [1] εκτελείται τουλάχιστον μία φορά ανά τρίμηνο.

— OVR-7.8-04 Η δοκιμή παρείσδυσης που απαιτείται από τη REQ-7.8-17X του ETSI EN 319 401 [1] εκτελείται τουλάχιστον μία φορά ετησίως.

— OVR-7.8-05 Τα τείχη προστασίας διαμορφώνονται έτσι ώστε να αποτρέπονται όλα τα πρωτόκολλα και οι προσβάσεις που δεν απαιτούνται για τη λειτουργία του παρόχου υπηρεσιών πληρωμών.

8) 7.14 Κρυπτογραφική παρακολούθηση

— OVR-7.14-03A Η αξιολόγηση των αλγορίθμων κρυπτογράφησης στις OVR-7.14.01 και OVR-7.14.02 συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

— ΣΗΜΕΙΩΣΗ άκυρο.

9) 7.12 Τερματισμός και σχέδια τερματισμού του παρόχου υπηρεσιών εμπιστοσύνης

— OVR-7.12-01A 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.2].

10) 7.17 Αλυσίδα εφοδιασμού

— OVR-7.17-01 Ισχύουν οι απαιτήσεις που ορίζονται στο ETSI EN 319 401 [1], σημείο 7.14.

11) Παράρτημα Α (κανονιστικό) Εγκεκριμένη υπηρεσία διαφύλαξης εγκεκριμένων ηλεκτρονικών υπογραφών, όπως ορίζεται στο άρθρο 34 του κανονισμού (ΕΕ) αριθ. 910/2014

— OVR-A-02 [PDS][PDS+PGD]

α) η υπηρεσία διαφύλαξης διαφυλάσσει όλες τις πληροφορίες που απαιτούνται για τον έλεγχο του χαρακτηρισμού της ηλεκτρονικής υπογραφής ή σφραγίδας ως εγκεκριμένης και οι οποίες δεν θα είναι διαθέσιμες στο κοινό έως το τέλος της περιόδου διαφύλαξης·

β) με την υπηρεσία διαφύλαξης διασφαλίζεται ότι, ανά πάσα στιγμή κατά τη διάρκεια της περιόδου διαφύλαξης, οι πληροφορίες που διαφυλάσσονται είναι τέτοιες ώστε, όταν παρέχονται ως δεδομένα για τη διαδικασία που ορίζεται στο σημείο 4.4 του ETSI TS 119 172-4 [9], το αποτέλεσμα της εν λόγω διαδικασίας προσδιορίζει σαφώς αν η ψηφιακή υπογραφή ή σφραγίδα ήταν, κατά τον χρόνο της διαφύλαξής της, τεχνικά κατάλληλη για την εφαρμογή εγκεκριμένης ηλεκτρονικής υπογραφής της ΕΕ ή εγκεκριμένης ηλεκτρονικής σφραγίδας της ΕΕ.

— OVR-A-03 [PDS][PDS+PGD] Οι χρονοσφραγίδες που χρησιμοποιούνται στα αποδεικτικά στοιχεία διαφύλαξης είναι εγκεκριμένες χρονοσφραγίδες σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014 [i.2].

2. Όσον αφορά το ETSI TS 119 172-4

1) 2.1 Κανονιστικές παραπομπές:

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Διαδικασίες για τη δημιουργία και την επικύρωση ψηφιακών υπογραφών AdES· Μέρος 1: Δημιουργία και επικύρωση».

— Όλες οι αναφορές στο «ETSI TS 119 102-1 [1]» νοούνται ως αναφορές στο «ETSI EN 319 102-1 [1]».

— [2] ETSI TS 119 612 (V2.3.1) «Ηλεκτρονικές Υπογραφές και Υποδομές (ESI)· Κατάλογοι εμπιστοσύνης».

— [13] ETSI TS 119 101 V1.1.1 (2016-03) «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Απαιτήσεις πολιτικής και ασφάλειας για τις αιτήσεις δημιουργίας υπογραφής και επικύρωσης υπογραφής».

2) 4.2 Περιορισμοί επικύρωσης και διαδικασίες επικύρωσης, απαίτηση REQ-4.2-03, ενότητα «X.509 περιορισμοί επικύρωσης», στοιχείο γ):

— i) Εάν ένα πιστοποιητικό οντότητας-τελικού αποδέκτη αντιπροσωπεύει άγκυρα εμπιστοσύνης, δεν χρησιμοποιούνται οι περιορισμοί «RevocationCheckingConstraints».

— ii) Εάν ένα πιστοποιητικό οντότητας-τελικού αποδέκτη δεν αντιπροσωπεύει άγκυρα εμπιστοσύνης, οι περιορισμοί «RevocationCheckingConstraints» ορίζονται ως «eitherCheck», όπως καθορίζεται στο ETSI TS 119 172-1 [3], σημείο A.4.2.1, πίνακας A.2 σειρές ιγ) 2.1.

— iii) Εάν ένα πιστοποιητικό οντότητας-τελικού αποδέκτη αντιπροσωπεύει άγκυρα εμπιστοσύνης, δεν χρησιμοποιούνται οι περιορισμοί «RevocationFreshnessConstraints» που καθορίζονται στο ETSI TS 119 172-1 [3], σημείο A.4.2.1 πίνακας A.2 σειρές ιγ) 2.2.

— iv) Εάν ένα πιστοποιητικό οντότητας-τελικού αποδέκτη δεν αντιπροσωπεύει άγκυρα εμπιστοσύνης, χρησιμοποιούνται οι περιορισμοί «RevocationFreshnessConstraints» που καθορίζονται στο ETSI TS 119 172-1 [3], σημείο A.4.2.1, πίνακας A.2 σειρές ιγ) 2.2, με μέγιστη τιμή 0 για το πιστοποιητικό υπογραφής, ώστε να διασφαλιστεί ότι οι πληροφορίες για την ανάκληση γίνονται δεκτές μόνο εάν έχουν εκδοθεί μετά τον βέλτιστο χρόνο υπογραφής. Δεν ορίζεται καμία τιμή για τους περιορισμούς «RevocationFreshnessConstraints» όταν πρόκειται για άλλα πιστοποιητικά εκτός του πιστοποιητικού υπογραφής, συμπεριλαμβανομένων των πιστοποιητικών που υποστηρίζουν χρονοσφραγίδες.

3) 4.3 Απαιτήσεις σχετικά με τις πρακτικές ελέγχου της επικύρωσης και των κανόνων εφαρμογής υπογραφής

— REQ-4.3-02 Οι αιτήσεις επικύρωσης υπογραφής συμμορφώνονται με το ETSI TS 119 101 [13].

4) 4.4 Διαδικασία ελέγχου της δυνατότητας τεχνικής εφαρμογής (κανόνες)

— REQ-4.4.2-03 Εάν οποιοσδήποτε από τους ελέγχους που προσδιορίζονται στη REQ-4.4.2-01 αποτύχει, τότε:

— η διαδικασία διακόπτεται·

— η υπογραφή προσδιορίζεται από τεχνική άποψη ως απροσδιόριστη, δηλαδή ούτε ως εγκεκριμένη ηλεκτρονική υπογραφή της ΕΕ ούτε ως εγκεκριμένη ηλεκτρονική σφραγίδα της ΕΕ·

— το ως άνω αποτέλεσμα και τα αποτελέσματα των διαδικασιών όλων των ενδιάμεσων διαδικασιών αποτυπώνονται στην έκθεση ελέγχου των κανόνων εφαρμογής υπογραφής.