Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/1929

30.9.2025

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/1929 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 τη σύνδεση της ημερομηνίας και της ώρας με τα δεδομένα και τον καθορισμό της ακρίβειας των χρονικών πηγών για την παροχή εγκεκριμένων ηλεκτρονικών χρονοσφραγίδων

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 42 παράγραφος 2,

Εκτιμώντας τα ακόλουθα:

(1) Οι εγκεκριμένες ηλεκτρονικές χρονοσφραγίδες διαδραματίζουν καίριο ρόλο στο ψηφιακό περιβάλλον, προωθώντας τη μετάβαση από τις παραδοσιακές έντυπες διαδικασίες σε ηλεκτρονικά ισοδύναμα. Συνδέοντας την ημερομηνία και την ώρα με τα ηλεκτρονικά δεδομένα, οι εγκεκριμένες ηλεκτρονικές χρονοσφραγίδες συμβάλλουν στη διασφάλιση της ακρίβειας της ημερομηνίας και της ώρας που αναγράφουν και της ακεραιότητας των ψηφιακών εγγράφων με τα οποία συνδέονται η ημερομηνία και η ώρα.

(2) Το τεκμήριο συμμόρφωσης που προβλέπεται στο άρθρο 42 παράγραφος 1α του κανονισμού (ΕΕ) αριθ. 910/2014 θα πρέπει να εφαρμόζεται μόνον όταν οι εγκεκριμένες υπηρεσίες εμπιστοσύνης για την έκδοση εγκεκριμένων χρονοσφραγίδων 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. Τα πρότυπα αυτά θα πρέπει να προσαρμοστούν ώστε να περιλαμβάνουν πρόσθετους ελέγχους που διασφαλίζουν την ασφάλεια και την αξιοπιστία των εγκεκριμένων υπηρεσιών εμπιστοσύνης και της σύνδεσης της ημερομηνίας και της ώρας με τα δεδομένα καθώς και της ακρίβειας της χρονικής πηγής.

(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 εκτελεστικό 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.

(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]).

([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).

([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.

(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

Τα πρότυπα αναφοράς και οι προδιαγραφές που αναφέρονται στο άρθρο 42 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 καθορίζονται στο παράρτημα του παρόντος κανονισμού.

Άρθρο 2

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

([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 για εγκεκριμένες υπηρεσίες χρονοσφραγίδων

Ισχύουν τα πρότυπα ETSI EN 319 421 V1.3.1 ([1]) («ETSI EN 319 421») και ETSI EN 319 422 V1.1.1 ([2]) («ETSI EN 319 422») με τις ακόλουθες προσαρμογές:

1. Όσον αφορά το ETSI EN 319 421

1) 2.1 Κανονιστικές παραπομπές:

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

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

— [5] ETSI EN 319 422 V1.1.1 (2016-03) «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Πρωτόκολλο χρονοσφράγισης και προφίλ αδειοπλαισίων χρονοσφραγίδων».

— [6] άκυρο.

— [9] 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]).

— [10] Εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής ([4]), 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).

— [11] Εκτελεστικός κανονισμός (ΕΕ) 2024/3144 ([5]) 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.

2) 3.1 Όροι

— Διάρκεια ισχύος πιστοποιητικού: χρονικό διάστημα από «notBefore» έως και «notAfter», κατά τη διάρκεια του οποίου η αρχή πιστοποίησης εγγυάται ότι θα διατηρεί τις πληροφορίες σχετικά με την κατάσταση του πιστοποιητικού.

3) 3.3 Συντομογραφίες

— EUCC Ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων

4) 6.2 Δήλωση πρακτικών υπηρεσιών εμπιστοσύνης

— OVR-6.2-03 Η αρχή χρονοσφράγισης συμπεριλαμβάνει δηλώσεις σχετικά με τη διαθεσιμότητα της υπηρεσίας χρονοσφράγισης στην οικεία δήλωση γνωστοποίησης αρχής χρονοσφράγισης.

5) 7.3 Ασφάλεια προσωπικού

— OVR-7.3-02 Τα μέλη του προσωπικού της αρχής χρονοσφράγισης 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-7.3-03 Η συμμόρφωση με το OVR-7.3-02 περιλαμβάνει τακτικές ενημερώσεις (τουλάχιστον κάθε 12 μήνες) σχετικά με τις νέες απειλές και τις τρέχουσες πρακτικές ασφάλειας.

([1]) EN 319 421 - Ηλεκτρονικές υπογραφές και υποδομές (ESI) - Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν χρονοσφραγίδες, V1.3.1.

([2]) EN 319 422 - Ηλεκτρονικές υπογραφές και υποδομές (ESI) - Πρωτόκολλο χρονοσφράγισης και προφίλ αδειοπλαισίων χρονοσφραγίδων, V1.1.1 (2016-03). https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.

([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

([4]) ΕΕ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

([5]) ΕΕ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Δημιουργία κλειδιών μονάδας χρονοσφράγισης

— TIS-7.6.2-03 Η δημιουργία του κλειδιού ή των κλειδιών μονάδας χρονοσφράγισης πραγματοποιείται 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 [3] 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 πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

β) EUCC [10][11], και πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

γ) έως τις 31.12.2030, το FIPS PUB 140-3 [7] 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 [10][11], τότε η διάταξη αυτή διαμορφώνεται και χρησιμοποιείται σύμφωνα με την εν λόγω πιστοποίηση.

— TIS-7.6.2-04 άκυρο.

— ΣΗΜΕΙΩΣΗ 3 άκυρο.

— TIS-7.6.2-05A Ο αλγόριθμος δημιουργίας κλειδιών μονάδας χρονοσφράγισης, το μήκος κλειδιού υπογραφής και ο αλγόριθμος υπογραφής που προκύπτουν, τα οποία χρησιμοποιούνται για την υπογραφή χρονοσφραγίδων και για την υπογραφή πιστοποιητικών δημόσιων κλειδιών μονάδας χρονοσφράγισης αντίστοιχα, συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας [9] και δημοσιεύει ο ENISA.

— ΣΗΜΕΙΩΣΗ 4 άκυρο.

— TIS-7.6.2-06 Το ιδιωτικό κλειδί υπογραφής μιας μονάδας χρονοσφράγισης 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) 7.6.3 Προστασία ιδιωτικού κλειδιού μονάδας χρονοσφράγισης

— TIS-7.6.3-02 Το ιδιωτικό κλειδί της μονάδας χρονοσφράγισης διατηρείται και χρησιμοποιείται 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 [3] ή στα κοινά κριτήρια για την αξιολόγηση της ασφάλειας της τεχνολογίας των πληροφοριών, έκδοση CC:2002, 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) το ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (στο εξής: EUCC) [10][11], και πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

γ) έως τις 31.12.2030, το FIPS PUB 140-3 [7] 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 [10][11], τότε η διάταξη αυτή διαμορφώνεται και χρησιμοποιείται σύμφωνα με την εν λόγω πιστοποίηση.

— TIS-7.6.3-03 άκυρο.

— ΣΗΜΕΙΩΣΗ 2 άκυρο.

8) 7.6.7 Τέλος του κύκλου ζωής του κλειδιού μονάδας χρονοσφράγισης

— TIS-7.6.7-03A Η ημερομηνία λήξης για τα ιδιωτικά κλειδιά μονάδας χρονοσφράγισης συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς [9].

— ΣΗΜΕΙΩΣΗ 1 άκυρο.

9) 7.10 Ασφάλεια δικτύου

— OVR-7.10-05 Η σάρωση τρωτών σημείων που απαιτείται από τη REQ-7.8-13 του ETSI EN 319 401 [1] εκτελείται τουλάχιστον μία φορά ανά τρίμηνο.

— OVR-7.10-06 Η δοκιμή παρείσδυσης που απαιτείται από τη REQ-7.8-17X του ETSI EN 319 401 [1] εκτελείται τουλάχιστον μία φορά ετησίως.

— OVR-7.10-07 Τα τείχη προστασίας διαμορφώνονται έτσι ώστε να αποτρέπονται όλα τα πρωτόκολλα και οι προσβάσεις που δεν απαιτούνται για τη λειτουργία της αρχής χρονοσφράγισης.

10) 7.14 Τερματισμός και σχέδια τερματισμού της αρχής χρονοσφράγισης

— OVR-7.14-01A 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.4].

2. Όσον αφορά το ETSI EN 319 422

1) 2.1 Κανονιστικές παραπομπές

— [5] άκυρο.

— [6] άκυρο.

— [8] Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, υποομάδα για την κρυπτογραφία: «Συμφωνημένοι κρυπτογραφικοί μηχανισμοί».

— [9] RFC 9110 Σημασιολογία HTTP.

2) 4.1.3 Αλγόριθμοι κατακερματισμού που πρέπει να χρησιμοποιούνται

— Ισχύει η ακόλουθη ρήτρα:

Οι αλγόριθμοι κατακερματισμού που χρησιμοποιούνται για τον κατακερματισμό των πληροφοριών που πρέπει να χρονοσφραγιστούν, η αναμενόμενη περίοδος διατήρησης της χρονοσφραγίδας και οι επιλεγμένες λειτουργίες κατακερματισμού σε σχέση με τον χρόνο συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

— ΣΗΜΕΙΩΣΗ άκυρο.

3) 4.2.3 Αλγόριθμοι που πρέπει να υποστηρίζονται

— Ισχύει η ακόλουθη ρήτρα:

Οι αλγόριθμοι υπογραφής των αδειοπλαισίων χρονοσφραγίδων που πρέπει να υποστηρίζονται συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

— ΣΗΜΕΙΩΣΗ άκυρο.

4) 4.2.4 Μήκη κλειδιών που πρέπει να υποστηρίζονται

— Ισχύει η ακόλουθη ρήτρα:

Τα μήκη κλειδιών αλγορίθμων υπογραφής για τον επιλεχθέντα αλγόριθμο υπογραφής συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA.

— ΣΗΜΕΙΩΣΗ άκυρο.

5) 5.1.3 Αλγόριθμοι που πρέπει να υποστηρίζονται

— Ισχύει η ακόλουθη ρήτρα:

Οι αλγόριθμοι κατακερματισμού για τα δεδομένα χρονοσφραγίδων που πρέπει να υποστηρίζονται, η αναμενόμενη περίοδος διατήρησης της χρονοσφραγίδας και οι επιλεγμένες λειτουργίες κατακερματισμού σε σχέση με τον χρόνο συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

— ΣΗΜΕΙΩΣΗ άκυρο.

6) 5.2.3 Αλγόριθμοι που πρέπει να χρησιμοποιούνται

— Ισχύει η ακόλουθη ρήτρα:

Οι αλγόριθμοι κατακερματισμού που χρησιμοποιούνται για τον κατακερματισμό των πληροφοριών που πρέπει να χρονοσφραγιστούν και οι αλγόριθμοι υπογραφής των αδειοπλαισίων χρονοσφραγίδων συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

— ΣΗΜΕΙΩΣΗ άκυρο.

7) 6.3 Απαιτήσεις όσον αφορά τα μήκη κλειδιών

— Ισχύει η ακόλουθη ρήτρα:

Το μήκος κλειδιού για τον επιλεχθέντα αλγόριθμο υπογραφής του πιστοποιητικού μονάδας χρονοσφράγισης συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

— ΣΗΜΕΙΩΣΗ άκυρο.

8) 6.5 Απαιτήσεις αλγορίθμων

— Ισχύει η ακόλουθη ρήτρα:

Το δημόσιο κλειδί μονάδας χρονοσφράγισης και η υπογραφή πιστοποιητικού μονάδας χρονοσφράγισης χρησιμοποιούν αλγόριθμους που συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

— ΣΗΜΕΙΩΣΗ άκυρο.

9) 7 Προφίλ για τα πρωτόκολλα μεταφοράς που πρέπει να υποστηρίζονται

— Ο πελάτης χρονοσφράγισης και ο εξυπηρετητής χρονοσφράγισης υποστηρίζουν το πρωτόκολλο χρονοσφράγισης μέσω HTTPS [9], όπως ορίζεται στο σημείο 3.4 του IETF RFC 3161 [1].

10) 8 Αναγνωριστικά αντικειμένου των αλγορίθμων κρυπτογράφησης

— Ισχύει η ακόλουθη ρήτρα:

Το δημόσιο κλειδί μονάδας χρονοσφράγισης και η υπογραφή πιστοποιητικού μονάδας χρονοσφράγισης χρησιμοποιούν αλγόριθμους σε συμμόρφωση με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [8].

11) 9.1 Δήλωση συμμόρφωσης με τον κανονισμό

— Εάν ένα αδειοπλαίσιο χρονοσφραγίδας δηλώνεται από την αρχή χρονοσφράγισης ως εγκεκριμένη ηλεκτρονική χρονοσφραγίδα σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014 [i.2], περιέχει μία περίπτωση της επέκτασης «QcStatements» στο πεδίο επέκτασης του αδειοπλαισίου χρονοσφραγίδας που συντάσσεται όπως ορίζεται στο IETF RFC 3739 [i.3], σημείο 3.2.6.

— Η επέκταση «QcStatements» περιλαμβάνει μία περίπτωση της δήλωσης «esi4-qtstStatement-1», όπως ορίζεται στο παράρτημα Β.

— Η επέκταση «QcStatements» δεν επισημαίνεται ως κρίσιμης σημασίας.