Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/1943

30.9.2025

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/1943 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 τα πρότυπα αναφοράς για τα εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών και τα εγκεκριμένα πιστοποιητικά 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 28 παράγραφος 6 και το άρθρο 38 παράγραφος 6,

Εκτιμώντας τα ακόλουθα:

(1) Τα εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών και τα εγκεκριμένα πιστοποιητικά ηλεκτρονικών σφραγίδων διαδραματίζουν καίριο ρόλο στο ψηφιακό επιχειρηματικό περιβάλλον, προωθώντας τη μετάβαση από τις παραδοσιακές έντυπες διαδικασίες σε ηλεκτρονικά ισοδύναμα. Με τη σύνδεση των δεδομένων επικύρωσης ηλεκτρονικής υπογραφής ή ηλεκτρονικής σφραγίδας με ένα φυσικό ή νομικό πρόσωπο αντίστοιχα και με την επιβεβαίωση του ονόματος του εν λόγω προσώπου, τα εγκεκριμένα πιστοποιητικά ενισχύουν τη βεβαιότητα όσον αφορά την ταυτότητα του υπογράφοντος και του δημιουργού της σφραγίδας.

(2) Το τεκμήριο συμμόρφωσης που προβλέπεται στο άρθρο 28 παράγραφος 6 και στο άρθρο 38 παράγραφος 6 του κανονισμού (ΕΕ) αριθ. 910/2014 θα πρέπει να εφαρμόζεται μόνο όταν οι εγκεκριμένες υπηρεσίες εμπιστοσύνης για την έκδοση εγκεκριμένων πιστοποιητικών ηλεκτρονικών υπογραφών και οι εγκεκριμένες υπηρεσίες εμπιστοσύνης για την έκδοση εγκεκριμένων πιστοποιητικών 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 των εγκεκριμένων υπηρεσιών εμπιστοσύνης και του περιεχομένου των εγκεκριμένων πιστοποιητικών.

(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.

(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

Πρότυπα αναφοράς και προδιαγραφές για εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών και ηλεκτρονικών σφραγίδων

1. Τα πρότυπα αναφοράς και οι προδιαγραφές που αναφέρονται στο άρθρο 28 παράγραφος 6 του κανονισμού (ΕΕ) αριθ. 910/2014 καθορίζονται στο παράρτημα I του παρόντος κανονισμού.

2. Τα πρότυπα αναφοράς και οι προδιαγραφές που αναφέρονται στο άρθρο 38 παράγραφος 6 του κανονισμού (ΕΕ) αριθ. 910/2014 καθορίζονται στο παράρτημα II 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

([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 Ι

Κατάλογος προτύπων αναφοράς και προδιαγραφών για εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών

Ισχύουν τα πρότυπα ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2») και ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5») με τις ακόλουθες προσαρμογές:

1. Όσον αφορά το ETSI EN 319 411-2

   1) 2.1 Κανονιστικές παραπομπές

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

      — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά· Μέρος 1: Γενικές απαιτήσεις», με τις ακόλουθες προσαρμογές:

        Το σημείο 2.1 Κανονιστικές παραπομπές του ETSI EN 319 411-1 V1.5.1 τροποποιείται ως εξής:

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

        — [10] ETSI EN 319 412-2 V2.4.1 «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Προφίλ πιστοποιητικών· Μέρος 2: Προφίλ πιστοποιητικού για πιστοποιητικά που εκδίδονται για φυσικά πρόσωπα».

        — [14] ETSI EN 319 412-1 V1.6.1 «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Προφίλ πιστοποιητικών· Μέρος 1: Επισκόπηση και κοινές δομές δεδομένων».

      — [3] ETSI EN 319 412-5 V2.5.1 «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Προφίλ πιστοποιητικών· Μέρος 5: QCStatements».

      — [5] ETSI EN 319 412-1 V1.6.1 «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Προφίλ πιστοποιητικών· Μέρος 1: Επισκόπηση και κοινές δομές δεδομένων».

      — [6] CEN/TS 419261:2015 «Απαιτήσεις ασφάλειας για αξιόπιστα συστήματα διαχείρισης πιστοποιητικών και χρονοσφραγίδων».

      — [7] 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) ([1]).

      — [8] Εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής ([2]) 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).

      — [9] Εκτελεστικός κανονισμός (ΕΕ) 2024/3144 της Επιτροπής ([3]) για την τροποποίηση του εκτελεστικού κανονισμού (ΕΕ) 2024/482 όσον αφορά τα εφαρμοστέα διεθνή πρότυπα και για τη διόρθωση του εν λόγω εκτελεστικού κανονισμού.

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

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

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

2) 5.2 Απαιτήσεις για τη δήλωση πρακτικών πιστοποίησης

— OVR-5.2-02 Η πολιτική ή οι πολιτικές πιστοποιητικών που προσδιορίζεται/-ονται στην τεκμηρίωση του παρόχου υπηρεσιών εμπιστοσύνης καθορίζει/-ουν τις απαιτήσεις σχετικά με τα προφίλ πιστοποιητικών που πρέπει να χρησιμοποιούνται.

3) 5.3 Ονομασία και ταυτοποίηση της πολιτικής πιστοποιητικών

— OVR-5.3-01 Εάν επέλθουν αλλαγές σε μια πολιτική πιστοποιητικών, όπως περιγράφεται στο σημείο 4.2.2, οι οποίες επηρεάζουν τη δυνατότητα εφαρμογής, τροποποιούνται τα αναγνωριστικά στοιχεία της πολιτικής.

4) 6.1 Ευθύνες δημοσιοποίησης και τήρησης αποθετηρίου

— OVR-6.1-02 Οι πληροφορίες που προσδιορίζονται στο DIS-6.1-04 του ETSI EN 319 411-1 [2] δημοσιοποιούνται και είναι διεθνώς διαθέσιμες.

5) 6.2.2 Αρχική επικύρωση ταυτότητας

— REG-6.2.2-01A Η συλλογή χαρακτηριστικών και αποδεικτικών στοιχείων σχετικά με την ταυτότητα του υποκειμένου, καθώς και η επικύρωσή τους, καθορίζονται σύμφωνα με τις εκτελεστικές πράξεις που εκδίδονται δυνάμει του άρθρου 24 παράγραφος 1γ του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] και [QCP-n-qscd] Η ταυτότητα του φυσικού προσώπου και, κατά περίπτωση, τυχόν ειδικά χαρακτηριστικά του προσώπου επαληθεύονται σύμφωνα με τις εκτελεστικές πράξεις που εκδίδονται δυνάμει του άρθρου 24 παράγραφος 1γ του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1].

— ΣΗΜΕΙΩΣΗ 1 άκυρο.

6) 6.3.3 Έκδοση πιστοποιητικού

— GEN-6.3.3-01 Ισχύουν οι απαιτήσεις GEN-6.3.3-01 έως GEN-6.3.3-10 που προσδιορίζονται στο ETSI EN 319 411-1 [2], σημείο 6.3.3.

— GEN-6.3.3-02 [ΥΠΟ ΟΡΟΥΣ] Εάν εκδοθεί πιστοποιητικό σε φυσικό πρόσωπο το οποίο ταυτοποιείται σε συνδυασμό με το νομικό πρόσωπο, τα χαρακτηριστικά του υποκειμένου που προσδιορίζουν τον οργανισμό στο πιστοποιητικό αντιπροσωπεύουν το νομικό πρόσωπο ή την υποοντότητα του εν λόγω νομικού προσώπου και τα αναγνωριστικά στοιχεία του υποκειμένου στο πιστοποιητικό αντιστοιχούν στο φυσικό πρόσωπο.

— GEN-6.3.3-03 Τα αναγνωριστικά στοιχεία της πολιτικής πιστοποιητικών είναι [ΕΠΙΛΟΓΗ]:

α) [QCP-n]

— όπως ορίζεται στο σημείο 5.3 στοιχείο α) και/ή

— αναγνωριστικό αντικειμένου, το οποίο χορηγείται από τον πάροχο υπηρεσιών εμπιστοσύνης, άλλο σχετικό ενδιαφερόμενο μέρος ή περαιτέρω τυποποίηση για πολιτική πιστοποιητικών που ενισχύει τις αντίστοιχες εφαρμοστέες απαιτήσεις πολιτικής που ορίζονται στο παρόν έγγραφο.

β) [QCP-n-qscd]

— όπως ορίζεται στο σημείο 5.3 στοιχείο γ) και/ή

— αναγνωριστικό αντικειμένου, το οποίο χορηγείται από τον πάροχο υπηρεσιών εμπιστοσύνης, άλλο σχετικό ενδιαφερόμενο μέρος ή περαιτέρω τυποποίηση για πολιτική πιστοποιητικών που ενισχύει τις αντίστοιχες εφαρμοστέες απαιτήσεις πολιτικής που ορίζονται στο παρόν έγγραφο.

7) 6.3.5 Χρήση ζεύγους κλειδιών και πιστοποιητικού

— SDP-6.3.5-02A [ΥΠΟ ΟΡΟΥΣ] Εάν ο πάροχος υπηρεσιών εμπιστοσύνης διαχειρίζεται την QSCD για το υποκείμενο, ο πάροχος υπηρεσιών εμπιστοσύνης είναι εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης που παρέχει εγκεκριμένη υπηρεσία εμπιστοσύνης για τη διαχείριση εγκεκριμένης διάταξης εξ αποστάσεως δημιουργίας ηλεκτρονικής υπογραφής, σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014 [i.1].

— SDP-6.3.5-11A Οι υποχρεώσεις του συνδρομητή (βλ. σημείο 6.3.4) περιλαμβάνουν, εάν ο συνδρομητής ή το υποκείμενο δημιουργεί τα κλειδιά του υποκειμένου:

α) υποχρέωση δημιουργίας των κλειδιών του υποκειμένου με τη χρήση αλγορίθμου που συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας [7] και δημοσιεύει ο ENISA για τις χρήσεις του πιστοποιημένου κλειδιού, όπως προσδιορίζονται στην πολιτική πιστοποιητικών·

β) υποχρέωση χρήσης μήκους κλειδιού και αλγορίθμου που συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας [7] και δημοσιεύει ο ENISA για τις χρήσεις του πιστοποιημένου κλειδιού, όπως προσδιορίζονται στην πολιτική πιστοποιητικών κατά τη διάρκεια ισχύος του πιστοποιητικού.

8) 6.3.10 Υπηρεσίες κατάστασης πιστοποιητικού

— CSS-6.3.10-08 [ΥΠΟ ΟΡΟΥΣ] Εάν παρέχονται κατάλογοι ανάκλησης πιστοποιητικών, ο πάροχος υπηρεσιών εμπιστοσύνης διατηρεί την ακεραιότητα και τη διαθεσιμότητα του τελευταίου καταλόγου ανάκλησης πιστοποιητικών τουλάχιστον για την περίοδο που ορίζεται στη δήλωση πρακτικών πιστοποίησης, όπως ζητείται στο CSS-6.3.10-12.

9) 6.4.4 Έλεγχοι προσωπικού

— OVR-6.4.4-02 Τα μέλη του προσωπικού του παρόχου υπηρεσιών εμπιστοσύνης 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-6.4.4-03 Η συμμόρφωση με το OVR-6.4.4-02 περιλαμβάνει τακτικές (τουλάχιστον κάθε 12 μήνες) ενημερώσεις σχετικά με τις νέες απειλές και τις τρέχουσες πρακτικές ασφάλειας.

— OVR-6.4.4-04 Πέραν των ρόλων εμπιστοσύνης που προσδιορίζονται στο ETSI EN 319 401 [1] (σημείο 7.2-15), υποστηρίζονται οι ρόλοι εμπιστοσύνης των υπευθύνων καταχώρισης και ανάκλησης που έχουν αναλάβει αρμοδιότητες οι οποίες ορίζονται στο TS 419261 [6]. Σε περιπτώσεις όπου ο εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης τελεί υπό την άμεση διαχείριση κράτους μέλους ή φορέα του δημόσιου τομέα ή λειτουργεί εξ ονόματός του, οι εν λόγω πρόσθετοι ρόλοι εμπιστοσύνης μπορούν να εκπληρώνονται από έναν ή περισσότερους επίσημους εκπροσώπους που ενεργούν εκ μέρους και για λογαριασμό των υπευθύνων καταχώρισης και ανάκλησης οι οποίοι υπηρετούν στις τοπικές ή περιφερειακές διοικήσεις.

10) 6.4.9 Τερματισμός της αρχής πιστοποίησης ή της αρχής καταχώρισης

— OVR-6.4,9-02 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].

11) 6.5.1 Δημιουργία και εγκατάσταση ζεύγους κλειδιών

— OVR-6.5.1-01A Η δημιουργία ζεύγους κλειδιών από την αρχή πιστοποίησης πραγματοποιείται με τη χρήση αλγορίθμου που συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [7] για τους σκοπούς της υπογραφής από την αρχή πιστοποίησης.

— OVR-6.5.1-01B Το μήκος κλειδιού και ο αλγόριθμος που επιλέγονται για το κλειδί υπογραφής της αρχής πιστοποίησης συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [7] για τους σκοπούς της υπογραφής από την αρχή πιστοποίησης.

— OVR-6.5.1-01C [ΥΠΟ ΟΡΟΥΣ] Εάν η αρχή πιστοποίησης δημιουργεί τα κλειδιά του υποκειμένου, τα κλειδιά του υποκειμένου που δημιουργούνται από την αρχή πιστοποίησης συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [7] για τους σκοπούς που αναφέρονται στην πολιτική πιστοποιητικών κατά τη διάρκεια ισχύος του πιστοποιητικού.

12) 6.5.2 Προστασία ιδιωτικών κλειδιών και έλεγχοι του σχεδιασμού του κρυπτογραφικού δομοστοιχείου

— GEN-6.5.2-01 Ισχύουν όλες οι απαιτήσεις που προσδιορίζονται στο ETSI EN 319 411-1 [2], σημείο 6.5.2, εκτός από τις απαιτήσεις OVR-6.5.2-01, OVR-6.5.2-03 και OVR-6.5.2-04.

— GEN-6.5.2-02 Η δημιουργία ζεύγους κλειδιών από τον πάροχο υπηρεσιών εμπιστοσύνης, συμπεριλαμβανομένων των κλειδιών που χρησιμοποιούνται από τις υπηρεσίες ανάκλησης και καταχώρισης, πραγματοποιείται εντός ασφαλούς κρυπτογραφικής διάταξης που συνιστά αξιόπιστο σύστημα πιστοποιημένο σύμφωνα με:

— 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: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

— το ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (στο εξής: EUCC) [8][9], και πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

— έως τις 31.12.2030, το FIPS PUB 140-3 [11] 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 [8][9], τότε η διάταξη αυτή διαμορφώνεται και χρησιμοποιείται σύμφωνα με την εν λόγω πιστοποίηση.

— GEN-6.5.2-03 Το ιδιωτικό κλειδί υπογραφής της αρχής πιστοποίησης διατηρείται και χρησιμοποιείται εντός ασφαλούς κρυπτογραφικής διάταξης που πληροί τις απαιτήσεις των GEN-6.5.2-01 και GEN-6.5.2-02.

13) 6.5.7 Έλεγχοι ασφάλειας δικτύου

— OVR-6.5.7-02 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-6.5.7-03 Η δοκιμή παρείσδυσης που απαιτείται από τη REQ-7.8-17X του ETSI EN 319 401 [1] εκτελείται τουλάχιστον μία φορά ετησίως.

— OVR-6.5.7-04 Τα τείχη προστασίας διαμορφώνονται έτσι ώστε να αποτρέπονται όλα τα πρωτόκολλα και οι προσβάσεις που δεν απαιτούνται για τη λειτουργία του παρόχου υπηρεσιών εμπιστοσύνης.

14) 6.6.1 Προφίλ πιστοποιητικού

— GEN-6.6.1-05 Το πιστοποιητικό περιλαμβάνει ένα από τα αναγνωριστικά στοιχεία πολιτικής που προσδιορίζονται στο GEN-6.3.3-03 [ΕΠΙΛΟΓΗ]. Το πιστοποιητικό μπορεί να περιλαμβάνει και άλλα αναγνωριστικά αντικειμένων που χορηγούνται από τον πάροχο υπηρεσιών εμπιστοσύνης.

2. Όσον αφορά το ETSI EN 319 412-2

1) 2.1 Κανονιστικές παραπομπές

— [2] ETSI EN 319 412-5 V2.5.1 «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Προφίλ πιστοποιητικών· Μέρος 5: QCStatements».

— [9] Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, υποομάδα για την κρυπτογραφία: «Συμφωνημένοι κρυπτογραφικοί μηχανισμοί» που δημοσιεύτηκε από τον ENISA.

2) 4.2.2 Υπογραφή

— GEN-4.2.2-2 Ο αλγόριθμος υπογραφής επιλέγεται σύμφωνα με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [9].

— ΣΗΜΕΙΩΣΗ άκυρο.

3) 4.2.3.1 Εκδότες-νομικά πρόσωπα

— GEN-4.2.3.1-3 Εάν είναι γνωστό ότι υπάρχει κατάλληλος αριθμός καταχώρισης, η ταυτότητα του εκδότη περιλαμβάνει χαρακτηριστικό «organizationIdentifier» το οποίο έχει την τιμή του εν λόγω αριθμού καταχώρισης, όπως αναφέρεται στο αντίστοιχο επίσημο αρχείο που καθορίζει τον εν λόγω αριθμό καταχώρισης.

4) 4.2.5 Πληροφορίες δημόσιου κλειδιού υποκειμένου

— GEN-4.2.5-2 Το δημόσιο κλειδί υποκειμένου επιλέγεται σύμφωνα με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [9].

— ΣΗΜΕΙΩΣΗ άκυρο.

5) 4.2.6 Αύξων αριθμός

— GEN-4.2.6-01 Ο αύξων αριθμός πιστοποιητικού (όπως ορίζεται στο IETF RFC 5280 [1] σημείο 4.1.2.2) είναι μοναδικός για κάθε πιστοποιητικό που εκδίδεται από τον πάροχο υπηρεσιών εμπιστοσύνης.

ΠΑΡΑΡΤΗΜΑ ΙΙ

Κατάλογος προτύπων αναφοράς και προδιαγραφών για εγκεκριμένα πιστοποιητικά ηλεκτρονικών σφραγίδων

Ισχύουν τα πρότυπα ETSI EN 319 411-2 V2.6.1 («ETSI EN 319 411-2»), ETSI EN 319 412-1 V1.6.1 («ETSI EN 319 412-1»), ETSI EN 319 412-3 V1.3.1 («ETSI EN 319 412-3»), ETSI EN 319 412-2 V2.4.1 («ETSI EN 319 412-2») και ETSI EN 319 412-5 V2.5.1 («ETSI EN 319 412-5») με τις ακόλουθες προσαρμογές:

1. Όσον αφορά το ETSI EN 319 411-2

   1) 2.1 Κανονιστικές παραπομπές

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

      — [2] ETSI EN 319 411-1 V1.5.1 (2025-04) «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά· Μέρος 1: Γενικές απαιτήσεις», με τις ακόλουθες προσαρμογές:

        Το σημείο 2.1 Κανονιστικές παραπομπές του ETSI EN 319 411-1 V1.5.1 τροποποιείται ως εξής:

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

        — [10] ETSI EN 319 412-2 V2.4.1 «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Προφίλ πιστοποιητικών· Μέρος 2: Προφίλ πιστοποιητικού για πιστοποιητικά που εκδίδονται για φυσικά πρόσωπα».

        — [14] ETSI EN 319 412-1 V1.6.1 «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Προφίλ πιστοποιητικών· Μέρος 1: Επισκόπηση και κοινές δομές δεδομένων».

      — [3] ETSI EN 319 412-5 V2.5.1 «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Προφίλ πιστοποιητικών· Μέρος 5: QCStatements».

      — [5] ETSI EN 319 412-1 V1.6.1 «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Προφίλ πιστοποιητικών· Μέρος 1: Επισκόπηση και κοινές δομές δεδομένων».

      — [6] CEN/TS 419261:2015 «Απαιτήσεις ασφάλειας για αξιόπιστα συστήματα διαχείρισης πιστοποιητικών και χρονοσφραγίδων» (που καταρτίστηκε από τη CEN).

      — [7] Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, υποομάδα για την κρυπτογραφία: «Συμφωνημένοι κρυπτογραφικοί μηχανισμοί» που δημοσιεύτηκε από τον ENISA.

      — [8] Εκτελεστικός κανονισμός (ΕΕ) 2024/482 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).

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

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

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

   2) 5.2 Απαιτήσεις για τη δήλωση πρακτικών πιστοποίησης

      — OVR-5.2-02 Η πολιτική ή οι πολιτικές πιστοποιητικών που προσδιορίζεται/-ονται στην τεκμηρίωση του παρόχου υπηρεσιών εμπιστοσύνης καθορίζει/-ουν τις απαιτήσεις σχετικά με τα προφίλ πιστοποιητικών που πρέπει να χρησιμοποιούνται.

3) 5.3 Ονομασία και ταυτοποίηση της πολιτικής πιστοποιητικών

— OVR-5.3-01 Εάν επέλθουν αλλαγές σε μια πολιτική πιστοποιητικών, όπως περιγράφεται στο σημείο 4.2.2, οι οποίες επηρεάζουν τη δυνατότητα εφαρμογής, τροποποιούνται τα αναγνωριστικά στοιχεία της πολιτικής.

4) 6.1 Ευθύνες δημοσιοποίησης και τήρησης αποθετηρίου

— OVR-6.1-02 Οι πληροφορίες που προσδιορίζονται στο DIS-6.1-04 του ETSI EN 319 411-1 [2] δημοσιοποιούνται και είναι διεθνώς διαθέσιμες.

5) 6.2.2 Αρχική επικύρωση ταυτότητας

— REG-6.2.2-01A Η συλλογή χαρακτηριστικών και αποδεικτικών στοιχείων σχετικά με την ταυτότητα του υποκειμένου, καθώς και η επικύρωσή τους, καθορίζονται σύμφωνα με τις εκτελεστικές πράξεις που εκδίδονται δυνάμει του άρθρου 24 παράγραφος 1γ του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1].

— REG-6.2.2-03 [QCP-l] και [QCP-l-qscd] Η ταυτότητα του νομικού προσώπου και, κατά περίπτωση, τυχόν ειδικά χαρακτηριστικά του προσώπου επαληθεύονται σύμφωνα με τις εκτελεστικές πράξεις που εκδίδονται δυνάμει του άρθρου 24 παράγραφος 1γ του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1].

— ΣΗΜΕΙΩΣΗ 3 Βλ. σημείωση 2.

6) 6.3.3 Έκδοση πιστοποιητικού

— GEN-6.3.3-01 Ισχύουν οι απαιτήσεις GEN-6.3.3-01 έως GEN-6.3.3-10 που προσδιορίζονται στο ETSI EN 319 411-1 [2], σημείο 6.3.3.

— GEN-6.3.3-02 Τα αναγνωριστικά στοιχεία της πολιτικής πιστοποιητικών είναι [ΕΠΙΛΟΓΗ]:

α) [QCP-l]

— όπως ορίζεται στο σημείο 5.3 στοιχείο β) και/ή

— αναγνωριστικό αντικειμένου, το οποίο χορηγείται από τον πάροχο υπηρεσιών εμπιστοσύνης, άλλο σχετικό ενδιαφερόμενο μέρος ή περαιτέρω τυποποίηση για πολιτική πιστοποιητικών που ενισχύει τις αντίστοιχες εφαρμοστέες απαιτήσεις πολιτικής που ορίζονται στο παρόν έγγραφο.

β) [QCP-l-qscd]

— όπως ορίζεται στο σημείο 5.3 στοιχείο δ) και/ή

— αναγνωριστικό αντικειμένου, που χορηγείται από τον πάροχο υπηρεσιών εμπιστοσύνης, άλλο σχετικό ενδιαφερόμενο μέρος ή περαιτέρω τυποποίηση για πολιτική πιστοποιητικών που ενισχύει τις εφαρμοστέες απαιτήσεις πολιτικής που ορίζονται στο παρόν έγγραφο.

7) 6.3.5 Χρήση ζεύγους κλειδιών και πιστοποιητικού

— SDP-6.3.5-02A [ΥΠΟ ΟΡΟΥΣ] Εάν ο πάροχος υπηρεσιών εμπιστοσύνης διαχειρίζεται την QSCD για το υποκείμενο, ο πάροχος υπηρεσιών εμπιστοσύνης είναι εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης που παρέχει εγκεκριμένη υπηρεσία εμπιστοσύνης για τη διαχείριση εγκεκριμένης διάταξης εξ αποστάσεως δημιουργίας ηλεκτρονικής σφραγίδας, σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014 [i.1].

— SDP-6.3.5-11A Οι υποχρεώσεις του συνδρομητή (βλ. σημείο 6.3.4) περιλαμβάνουν, εάν ο συνδρομητής ή το υποκείμενο δημιουργεί τα κλειδιά του υποκειμένου:

α) υποχρέωση δημιουργίας των κλειδιών του υποκειμένου με τη χρήση αλγορίθμου που συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [7] για τις χρήσεις του πιστοποιημένου κλειδιού, όπως προσδιορίζονται στην πολιτική πιστοποιητικών· και

β) υποχρέωση χρήσης μήκους κλειδιού και αλγορίθμου που συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [7] για τις χρήσεις του πιστοποιημένου κλειδιού, όπως προσδιορίζονται στην πολιτική πιστοποιητικών κατά τη διάρκεια ισχύος του πιστοποιητικού.

8) 6.3.10 Υπηρεσίες κατάστασης πιστοποιητικού

— CSS-6.3.10-08 [ΥΠΟ ΟΡΟΥΣ] Εάν παρέχονται κατάλογοι ανάκλησης πιστοποιητικών, ο πάροχος υπηρεσιών εμπιστοσύνης διατηρεί την ακεραιότητα και τη διαθεσιμότητα του τελευταίου καταλόγου ανάκλησης πιστοποιητικών τουλάχιστον για την περίοδο που ορίζεται στη δήλωση πρακτικών πιστοποίησης, όπως ζητείται στο CSS-6.3.10-12.

9) 6.4.4 Έλεγχοι προσωπικού

— OVR-6.4.4-02 Τα μέλη του προσωπικού του παρόχου υπηρεσιών εμπιστοσύνης 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-6.4.4-03 Η συμμόρφωση με το OVR-6.4.4-02 περιλαμβάνει τακτικές ενημερώσεις (τουλάχιστον κάθε 12 μήνες) σχετικά με τις νέες απειλές και τις τρέχουσες πρακτικές ασφάλειας.

— OVR-6.4.4-04 Πέραν των ρόλων εμπιστοσύνης που προσδιορίζονται στο ETSI EN 319 401 [1] (σημείο 7.2-15), υποστηρίζονται οι ρόλοι εμπιστοσύνης των υπευθύνων καταχώρισης και ανάκλησης που έχουν αναλάβει αρμοδιότητες οι οποίες ορίζονται στο TS 419261 [6]. Σε περιπτώσεις όπου ο εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης τελεί υπό την άμεση διαχείριση κράτους μέλους ή φορέα του δημόσιου τομέα ή λειτουργεί εξ ονόματός του, οι εν λόγω πρόσθετοι ρόλοι εμπιστοσύνης μπορούν να εκπληρώνονται από έναν ή περισσότερους επίσημους εκπροσώπους που ενεργούν εκ μέρους και για λογαριασμό των υπευθύνων καταχώρισης και ανάκλησης οι οποίοι υπηρετούν στις τοπικές ή περιφερειακές διοικήσεις.

10) 6.4.9 Τερματισμός της αρχής πιστοποίησης ή της αρχής καταχώρισης

— OVR-6.4,9-02 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].

11) 6.5.1 Δημιουργία και εγκατάσταση ζεύγους κλειδιών

— OVR-6.5.1-01A Η δημιουργία ζεύγους κλειδιών από την αρχή πιστοποίησης πραγματοποιείται με τη χρήση αλγορίθμου που συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [7] για τους σκοπούς της υπογραφής από την αρχή πιστοποίησης.

— OVR-6.5.1-01B Το μήκος κλειδιού και ο αλγόριθμος που επιλέγονται για το κλειδί υπογραφής της αρχής πιστοποίησης συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [7] για τους σκοπούς της υπογραφής από την αρχή πιστοποίησης.

— OVR-6.5.1-01C [ΥΠΟ ΟΡΟΥΣ] Εάν η αρχή πιστοποίησης δημιουργεί τα κλειδιά του υποκειμένου, τα κλειδιά του υποκειμένου που δημιουργούνται από την αρχή πιστοποίησης συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [7] για τους σκοπούς που αναφέρονται στην πολιτική πιστοποιητικών κατά τη διάρκεια ισχύος του πιστοποιητικού.

12) 6.5.2 Προστασία ιδιωτικών κλειδιών και έλεγχοι του σχεδιασμού του κρυπτογραφικού δομοστοιχείου

— GEN-6.5.2-01 Ισχύουν όλες οι απαιτήσεις που προσδιορίζονται στο ETSI EN 319 411-1 [2], σημείο 6.5.2, εκτός από τις απαιτήσεις OVR-6.5.2-01, OVR-6.5.2-03 και OVR-6.5.2-04.

— GEN-6.5.2-02 Η δημιουργία ζεύγους κλειδιών από τον πάροχο υπηρεσιών εμπιστοσύνης, συμπεριλαμβανομένων των κλειδιών που χρησιμοποιούνται από τις υπηρεσίες ανάκλησης και καταχώρισης, πραγματοποιείται εντός ασφαλούς κρυπτογραφικής διάταξης που συνιστά αξιόπιστο σύστημα πιστοποιημένο σύμφωνα με:

  — 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: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

  — το ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων (στο εξής: EUCC) [8][9], και πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

  — έως τις 31.12.2030, το FIPS PUB 140-3 [11] 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 [8][9], τότε η διάταξη αυτή διαμορφώνεται και χρησιμοποιείται σύμφωνα με την εν λόγω πιστοποίηση.

— GEN-6.5.2-03 Το ιδιωτικό κλειδί υπογραφής της αρχής πιστοποίησης διατηρείται και χρησιμοποιείται εντός ασφαλούς κρυπτογραφικής διάταξης που πληροί τις απαιτήσεις των GEN-6.5.2-01 και GEN-6.5.2-02.

13) 6.5.7 Έλεγχοι ασφάλειας δικτύου

— OVR-6.5.7-02 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-6.5.7-03 Η δοκιμή παρείσδυσης που απαιτείται από τη REQ-7.8-17X του ETSI EN 319 401 [1] εκτελείται τουλάχιστον μία φορά ετησίως.

— OVR-6.5.7-04 Τα τείχη προστασίας διαμορφώνονται έτσι ώστε να αποτρέπονται όλα τα πρωτόκολλα και οι προσβάσεις που δεν απαιτούνται για τη λειτουργία του παρόχου υπηρεσιών εμπιστοσύνης.

14) 6.6.1 Προφίλ πιστοποιητικού

— GEN-6.6.1-05 Το πιστοποιητικό περιλαμβάνει ένα από τα αναγνωριστικά στοιχεία πολιτικής που προσδιορίζονται στο GEN-6.3.3-02 [ΕΠΙΛΟΓΗ].

2. Όσον αφορά το ETSI EN 319 412-3

1) 2.1 Κανονιστικές παραπομπές

— [2] ETSI EN 319 412-2 V2.4.1 «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Προφίλ πιστοποιητικών· Μέρος 2: Προφίλ πιστοποιητικού για πιστοποιητικά που εκδίδονται για φυσικά πρόσωπα».

2) 4.2.1 Υποκείμενο

— LEG-4.2.1-6 Το χαρακτηριστικό «organizationIdentifier» περιέχει ταυτοποίηση του υποκειμένου-οργανισμού διαφορετική από την επωνυμία του οργανισμού. Εάν είναι γνωστό ότι υπάρχει κατάλληλος αριθμός καταχώρισης, το χαρακτηριστικό «organizationIdentifier» περιλαμβάνει τιμή του εν λόγω αριθμού καταχώρισης, όπως αναφέρεται στο αντίστοιχο επίσημο αρχείο που καθορίζει τον εν λόγω αριθμό καταχώρισης.

3. Όσον αφορά το ETSI EN 319 412-2:

1) 2.1 Κανονιστικές παραπομπές

— [2] ETSI EN 319 412-5 V2.5.1 «Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Προφίλ πιστοποιητικών· Μέρος 5: QCStatements».

— [9] Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, υποομάδα για την κρυπτογραφία: «Συμφωνημένοι κρυπτογραφικοί μηχανισμοί» που δημοσιεύτηκε από τον ENISA.

2) 2.2 Ενημερωτικές παραπομπές

— [I.7] άκυρο.

3) 4.2.2 Υπογραφή

— GEN-4.2.2-2 Ο αλγόριθμος υπογραφής επιλέγεται σύμφωνα με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [9].

— ΣΗΜΕΙΩΣΗ άκυρο.

4) 4.2.3.1 Εκδότες-νομικά πρόσωπα

— GEN-4.2.3.1-3 Εάν είναι γνωστό ότι υπάρχει κατάλληλος αριθμός καταχώρισης, η ταυτότητα του εκδότη περιλαμβάνει χαρακτηριστικό «organizationIdentifier» το οποίο έχει την τιμή του εν λόγω αριθμού καταχώρισης, όπως αναφέρεται στο αντίστοιχο επίσημο αρχείο που καθορίζει τον εν λόγω αριθμό καταχώρισης.

5) 4.2.5 Πληροφορίες δημόσιου κλειδιού υποκειμένου

— GEN-4.2.5-2 Το δημόσιο κλειδί υποκειμένου επιλέγεται σύμφωνα με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [9].

— ΣΗΜΕΙΩΣΗ άκυρο.

6) 4.2.6 Αύξων αριθμός

— GEN-4.2.6-01 Ο αύξων αριθμός πιστοποιητικού (όπως ορίζεται στο IETF RFC 5280 [1] σημείο 4.1.2.2) είναι μοναδικός για κάθε πιστοποιητικό που εκδίδεται από τον πάροχο υπηρεσιών εμπιστοσύνης.