Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/1942

30.9.2025

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/1942 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 επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών και τις εγκεκριμένες υπηρεσίες επικύρωσης 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 33 παράγραφος 2 και το άρθρο 40,

Εκτιμώντας τα ακόλουθα:

(1) Οι εγκεκριμένες υπηρεσίες επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών και εγκεκριμένων ηλεκτρονικών σφραγίδων διασφαλίζουν την ακεραιότητα, τη γνησιότητα και την ορθότητα της διαδικασίας και των αποτελεσμάτων της επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών και εγκεκριμένων ηλεκτρονικών σφραγίδων αντίστοιχα. Οι εν λόγω ηλεκτρονικές υπηρεσίες εμπιστοσύνης διαδραματίζουν καίριο ρόλο στο ψηφιακό επιχειρηματικό περιβάλλον, προωθώντας τη μετάβαση από τις παραδοσιακές έντυπες διαδικασίες σε ηλεκτρονικά ισοδύναμα.

(2) Το τεκμήριο συμμόρφωσης που προβλέπεται στο άρθρο 33 παράγραφος 2 και στο άρθρο 40 του κανονισμού (ΕΕ) αριθ. 910/2014 θα πρέπει να εφαρμόζεται μόνο όταν οι εγκεκριμένες υπηρεσίες επικύρωσης 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 των εγκεκριμένων υπηρεσιών εμπιστοσύνης, καθώς και την ικανότητα επαλήθευσης του χαρακτηρισμού των ηλεκτρονικών υπογραφών και των ηλεκτρονικών σφραγίδων ως εγκεκριμένων, αφενός, και της τεχνικής εγκυρότητάς τους, 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 33 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 για εγκεκριμένες υπηρεσίες επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών και εγκεκριμένες υπηρεσίες επικύρωσης εγκεκριμένων ηλεκτρονικών σφραγίδων

Ισχύουν τα πρότυπα ETSI TS 119 441 V1.2.1 (2023-10) ([1]) («ETSI TS 119 441») και ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) («ETSI TS 119 172-4») με τις ακόλουθες προσαρμογές:

1. Όσον αφορά το ETSI TS 119 441

1) 2.1 Κανονιστικές παραπομπές

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

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

— [4] ISO/IEC 15408-1:2022 – Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικότητας – Κριτήρια αξιολόγησης για την ασφάλεια της τεχνολογίας πληροφοριών.

— [5] άκυρο.

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

— [7] Εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής ([3]) 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).

— [8] 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».

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Διαδικασίες για τη δημιουργία και την επικύρωση ψηφιακών υπογραφών AdES· Μέρος 2: Έκθεση επικύρωσης υπογραφής».

— [10] 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) ([4]).

— [11] Εκτελεστικός κανονισμός (ΕΕ) 2024/3144 της Επιτροπής ([5]) για την τροποποίηση του εκτελεστικού κανονισμού (ΕΕ) 2024/4822 όσον αφορά τα εφαρμοστέα διεθνή πρότυπα και για τη διόρθωση του εν λόγω εκτελεστικού κανονισμού.

— [12] ETSI EN 319 411-1 «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά· Μέρος 1: Γενικές απαιτήσεις».

([1]) ETSI TS 119 441 - Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Απαιτήσεις πολιτικής για παρόχους υπηρεσιών εμπιστοσύνης που παρέχουν υπηρεσίες επικύρωσης υπογραφής, V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 - 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, V1.1.1 (2021-05).
([3]) ΕΕ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([5]) ΕΕ L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Ενημερωτικές παραπομπές

— [i.11] άκυρο.

3) 3.3 Συντομογραφίες

— EUCC Ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας βάσει κοινών κριτηρίων

4) 4.3.3. Διαδικασία

— ΣΗΜΕΙΩΣΗ 10 Βλ. ETSI EN 319 102-1 [3] για οδηγίες και ETSI TS 119 172-4 [8] για πρόσθετες οδηγίες σχετικά με την περίπτωση της εγκεκριμένης υπογραφής ή σφραγίδας της ΕΕ.

5) 6.1 Δήλωση πρακτικών της υπηρεσίας επικύρωσης υπογραφής (στο εξής: SVS)

— OVR-6.1-02 Η δήλωση πρακτικών SVS διαρθρώνεται σύμφωνα με το παράρτημα Α.

— OVR-6.1-03 Η δήλωση πρακτικών SVS απαριθμεί τις υποστηριζόμενες πολιτικές SVS ή παραπέμπει σε αυτές (π.χ. μέσω αναγνωριστικού αντικειμένου) και τις περιγράφει εν συντομία.

6) 6.3 Πολιτική ασφάλειας πληροφοριών

— OVR-6.3-02 Η πολιτική ασφάλειας τεκμηριώνει τους ελέγχους ασφάλειας και ιδιωτικότητας που εφαρμόζονται για την προστασία των δεδομένων προσωπικού χαρακτήρα.

7) 7.2 Ανθρώπινοι πόροι

— OVR-7.2-02 Τα μέλη του προσωπικού του SVSP 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.

8) 7.5 Κρυπτογραφικοί έλεγχοι

— OVR-7.5-02 [ΥΠΟ ΟΡΟΥΣ] Όταν υπογράφονται εκθέσεις επικύρωσης, το δημόσιο πιστοποιητικό υπογραφής του SVSP που αντιστοιχεί στο ιδιωτικό κλειδί υπογραφής του SVSP εκδίδεται, από αξιόπιστη αρχή πιστοποίησης, σύμφωνα με την πολιτική πιστοποιητικών (NCP+), όπως ορίζεται στο ETSI EN 319 411-1 [12]. Θα πρέπει να εκδίδεται σύμφωνα με κατάλληλη πολιτική πιστοποιητικών που ορίζεται στο ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [ΥΠΟ ΟΡΟΥΣ] Όταν υπογράφονται εκθέσεις επικύρωσης, το ιδιωτικό κλειδί υπογραφής του SVSP 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 [4] 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 [7][11], και πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

γ) έως τις 31.12.2030, το FIPS PUB 140-3 [6] 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 [7][11], τότε η διάταξη αυτή διαμορφώνεται και χρησιμοποιείται σύμφωνα με την εν λόγω πιστοποίηση.

— OVR-7.5-04 άκυρο.

— OVR-7.5-06 Το ιδιωτικό κλειδί υπογραφής ενός SVSP 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.

9) 7.7 Ασφάλεια λειτουργίας

— OVR-7.7-02 Προκειμένου να διασφαλιστεί ότι τα συστήματα στα οποία αναπτύσσεται η εφαρμογή εφαρμόζουν κατάλληλα μέτρα ασφάλειας και προσαρμόζονται σε ειδικά περιβάλλοντα εφαρμογών, η SVA χρησιμοποιεί περιβάλλον εφαρμογής που συντηρείται με επικαιροποιημένες διορθωτικές ρυθμίσεις ασφάλειας.

— OVR-7.7-03 Όσον αφορά την SVA ισχύουν οι ακόλουθες απαιτήσεις που ορίζονται στο ETSI EN 119 101 [1], σημείο 5.2: GSM 1.3.

10) 7.8 Ασφάλεια δικτύου

— OVR-7.8-02 Εάν επιτρέπεται η εξ αποστάσεως πρόσβαση σε συστήματα αποθήκευσης ή επεξεργασίας εμπιστευτικών δεδομένων, εγκρίνεται επίσημη πολιτική η οποία περιγράφεται ως μέρος των στοιχείων που απαιτούνται από την OVR-6.3-02.

— OVR-7.8-04 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-7.8-05 Η δοκιμή παρείσδυσης που απαιτείται από τη REQ-7.8-17X του ETSI EN 319 401 [1] εκτελείται τουλάχιστον μία φορά ετησίως.

— OVR-7.8-06: Τα τείχη προστασίας διαμορφώνονται έτσι ώστε να αποτρέπονται όλα τα πρωτόκολλα και οι προσβάσεις που δεν απαιτούνται για τη λειτουργία του SVSP.

11) 7.12 Τερματισμός και σχέδια τερματισμού της παροχής υπηρεσιών επικύρωσης υπογραφής

— OVR-7.12-02 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].

12) 7.14 Αλυσίδα εφοδιασμού

— OVR-7.14-01 Ισχύουν οι απαιτήσεις που ορίζονται στο ETSI EN 319 401 [2], σημείο 7.14.

13) 8.1 Διαδικασία επικύρωσης υπογραφής

— VPR-8.1-07 Η αίτηση επικύρωσης (SVA) συμμορφώνεται με τις απαιτήσεις του ETSI TS 119 101 [1], σημείο 7.4 SIA 1 έως SIA 4.

— VPR-8.1-11 [ΥΠΟ ΟΡΟΥΣ] Όταν η SVS αποσκοπεί στην επικύρωση εγκεκριμένων ηλεκτρονικών υπογραφών ή εγκεκριμένων ηλεκτρονικών σφραγίδων σύμφωνα με το άρθρο 32 παράγραφος 1 (ή το άρθρο 40 αντίστοιχα) του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1], η διαδικασία επικύρωσης ακολουθεί τις απαιτήσεις του ETSI TS 119 172-4 [8].

14) 8.2 Πρωτόκολλο επικύρωσης υπογραφής

— SVP-8.2-03 Η απάντηση επικύρωσης υπογραφής φέρει το αναγνωριστικό αντικειμένου της πολιτικής SVS.

15) 8.4 Έκθεση επικύρωσης υπογραφής

— SVR-8.4-02 Η έκθεση επικύρωσης συμμορφώνεται με το ETSI TS 119 102-2 [9].

— SVR-8.4-07 [ΥΠΟ ΟΡΟΥΣ] Όταν η πολιτική επικύρωσης υπογραφής δεν διεκπεραιώνεται πλήρως στο πλαίσιο της SVS, η έκθεση, πέραν της αναφοράς σχετικά με επικυρωμένους περιορισμούς, αναφέρει τους περιορισμούς που αγνοήθηκαν ή παρακάμφθηκαν.

— SVR-8.4-15 Η έκθεση επικύρωσης αναφέρει σαφώς την προέλευση κάθε απόδειξης ύπαρξης (PoE) (από το εσωτερικό της υπογραφής, από τον πελάτη, από τον εξυπηρετητή).

— SVR-8.4-16 Η έκθεση επικύρωσης φέρει υπογραφή έκθεσης επικύρωσης, η οποία είναι η ψηφιακή υπογραφή του SVSP.

— SVR-8.4-17 [ΥΠΟ ΟΡΟΥΣ] Όταν υπογράφονται οι εκθέσεις επικύρωσης, ο μορφότυπος και ο στόχος της υπογραφής συμμορφώνονται με το ETSI TS 119 102-2 [9].

16) 9 Πλαίσιο για τον καθορισμό πολιτικών υπηρεσιών επικύρωσης με βάση πολιτική υπηρεσίας εμπιστοσύνης που ορίζεται στο παρόν έγγραφο:

— OVR-9-05 [ΥΠΟ ΟΡΟΥΣ] Κατά τη χάραξη πολιτικής SVS με βάση πολιτική υπηρεσίας εμπιστοσύνης που ορίζεται στο παρόν έγγραφο, διενεργείται εκτίμηση κινδύνου για την αξιολόγηση των επιχειρηματικών απαιτήσεων και τον καθορισμό των απαιτήσεων ασφάλειας που πρέπει να συμπεριληφθούν στην πολιτική για τη δηλωμένη κοινότητα και δυνατότητα εφαρμογής.

— OVR-9-06 [ΥΠΟ ΟΡΟΥΣ] Κατά τη χάραξη πολιτικής SVS με βάση πολιτική υπηρεσίας εμπιστοσύνης που ορίζεται στο παρόν έγγραφο, η πολιτική εγκρίνεται και τροποποιείται σύμφωνα με καθορισμένη διαδικασία επανεξέτασης, συμπεριλαμβανομένων των ευθυνών για τη διατήρηση της πολιτικής.

— OVR-9-07 [ΥΠΟ ΟΡΟΥΣ] Κατά τη χάραξη πολιτικής SVS με βάση πολιτική υπηρεσίας εμπιστοσύνης που ορίζεται στο παρόν έγγραφο, πρέπει να υπάρχει καθορισμένη διαδικασία επανεξέτασης ώστε να διασφαλίζεται ότι η πολιτική υποστηρίζεται από τις δηλώσεις πρακτικών.

— OVR-9-08 [ΥΠΟ ΟΡΟΥΣ] Κατά τη χάραξη πολιτικής SVS με βάση πολιτική υπηρεσίας εμπιστοσύνης που ορίζεται στο παρόν έγγραφο, ο πάροχος υπηρεσιών εμπιστοσύνης καθιστά διαθέσιμες τις πολιτικές που υποστηρίζονται από τον πάροχο υπηρεσιών εμπιστοσύνης στην κοινότητα χρηστών του.

— OVR-9-09 [ΥΠΟ ΟΡΟΥΣ] Κατά τη χάραξη πολιτικής SVS με βάση πολιτική υπηρεσίας εμπιστοσύνης που ορίζεται στο παρόν έγγραφο, οι αναθεωρήσεις των πολιτικών που υποστηρίζονται από τον πάροχο υπηρεσιών εμπιστοσύνης τίθενται στη διάθεση των συνδρομητών.

17) Παράρτημα Β (κανονιστικό) Εγκεκριμένη υπηρεσία επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών, όπως ορίζεται στο άρθρο 33 του κανονισμού (ΕΕ) αριθ. 910/2014:

— VPR-B-02 [ΥΠΟ ΟΡΟΥΣ] Εάν ο SVSP είναι εγκεκριμένος πάροχος υπηρεσιών επικύρωσης υπογραφής (στο εξής: QSVSP), η υλοποίηση συμμορφώνεται με το ETSI TS 119 172-4 [8].

— ΣΗΜΕΙΩΣΗ 2 άκυρο.

— OVR-B-04 [ΥΠΟ ΟΡΟΥΣ] Εάν ο SVSP είναι QSVSP, με τις δοκιμές στην OVR-B-03 ελέγχονται διαφορετικές περιπτώσεις χρήσης, θετικές και αρνητικές.

— VPR-B-11 [ΥΠΟ ΟΡΟΥΣ] Εάν ο SVSP είναι QSVSP, ο SVSP ελέγχει τον υπολογισμό κατακερματισμού (είτε εκτελεί τον υπολογισμό στην πλευρά του εξυπηρετητή είτε ελέγχει τον πελάτη εάν επιτρέπεται από την πλευρά του πελάτη).

— ΣΗΜΕΙΩΣΗ 5 άκυρο.

— ΣΗΜΕΙΩΣΗ 6 άκυρο.

— VPR-B-15 [ΥΠΟ ΟΡΟΥΣ] Εάν ο SVSP είναι QSVSP, προκειμένου να πληρούνται οι VPR-B-13 έως VPR-B-14, η έκθεση επικύρωσης συμμορφώνεται με το ETSI TS 119 102-2 [9].

— VPR-B-16 [ΥΠΟ ΟΡΟΥΣ] Εάν ο SVSP είναι QSVSP, η υλοποίηση συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [10] για τη χρήση κατάλληλων κρυπτογραφικών τεχνικών κατά την παροχή εγκεκριμένων υπηρεσιών επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών.

18) ΠΑΡΑΡΤΗΜΑ Γ (πληροφοριακό) Χαρτογράφηση των απαιτήσεων του κανονισμού (ΕΕ) αριθ. 910/2014, τμήμα «Παροχή επικύρωσης σύμφωνα με το άρθρο 32 παράγραφος 1» δεύτερο εδάφιο:

— Προκειμένου να διασφαλιστεί ότι επαληθεύονται όλες οι προϋποθέσεις που απαιτούνται από το άρθρο 32 παράγραφος 1 και το άρθρο 40 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1], απαιτείται ορθός αλγόριθμος επικύρωσης. Ο εν λόγω αλγόριθμός παρέχει το ίδιο προσδιοριστικό αποτέλεσμα για την υπογραφή ή τη σφραγίδα που υποβάλλεται προς επικύρωση. Η πολιτική επικύρωσης υπογραφής είναι ζωτικής σημασίας για τον σκοπό αυτόν. Το ETSI TS 119 172-4 [8], με βάση τον αλγόριθμο επικύρωσης που καθορίζεται στο ETSI EN 319 102-1 [3], εκδόθηκε με την προοπτική αυτή.

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 (2024-11) «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 24 ώρες για το πιστοποιητικό 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) 4.4 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:

α) η διαδικασία διακόπτεται·

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

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