Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2025/1944

30.9.2025

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2025/1944 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 διαδικασίες αποστολής και λήψης δεδομένων στο πλαίσιο εγκεκριμένων ηλεκτρονικών υπηρεσιών συστημένης παράδοσης και όσον αφορά τη διαλειτουργικότητα των εν λόγω υπηρεσιών

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 44 παράγραφος 2 και το άρθρο 44 παράγραφος 2β,

Εκτιμώντας τα ακόλουθα:

(1) Οι εγκεκριμένες ηλεκτρονικές υπηρεσίες συστημένης παράδοσης παρέχουν ασφαλή δίαυλο για τη διαβίβαση εγγράφων, με απόδειξη αποστολής και παραλαβής των δεδομένων. Αποσκοπούν στη διασφάλιση βεβαιότητας όσον αφορά την ταυτοποίηση του αποδέκτη και εξασφαλίζουν υψηλό επίπεδο εμπιστοσύνης όσον αφορά την ταυτοποίηση του αποστολέα.

(2) Το τεκμήριο συμμόρφωσης που προβλέπεται στο άρθρο 44 παράγραφος 1α του κανονισμού (ΕΕ) αριθ. 910/2014 θα πρέπει να εφαρμόζεται μόνο όταν οι εγκεκριμένες υπηρεσίες εμπιστοσύνης για την παροχή εγκεκριμένων ηλεκτρονικών υπηρεσιών συστημένης παράδοσης 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.

(3) Εάν ένας πάροχος υπηρεσιών εμπιστοσύνης συμμορφώνεται με τις απαιτήσεις που ορίζονται στο παράρτημα Ι 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) Σύμφωνα με το άρθρο 44 παράγραφος 2α του κανονισμού (ΕΕ) αριθ. 910/2014, όταν οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης συμφωνούν να καταστήσουν τις υπηρεσίες τους διαλειτουργικές, είναι σημαντικό να τηρούν τα κατάλληλα πρότυπα και τις κατάλληλες προδιαγραφές που ορίζονται στο παράρτημα ΙΙ του παρόντος εκτελεστικού κανονισμού, προκειμένου να διαβιβάζονται εύκολα τα ηλεκτρονικά καταχωρισμένα δεδομένα μεταξύ δύο ή περισσότερων εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης και να προωθούνται θεμιτές πρακτικές στην εσωτερική αγορά.

(5) 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).

(6) Σε όλες τις 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]).

(7) 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.

(8) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 48 του κανονισμού (ΕΕ) αριθ. 910/2014,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Πρότυπα αναφοράς και προδιαγραφές για εγκεκριμένες ηλεκτρονικές υπηρεσίες συστημένης παράδοσης

Τα πρότυπα αναφοράς και οι προδιαγραφές που αναφέρονται στο άρθρο 44 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 καθορίζονται στο παράρτημα Ι του παρόντος κανονισμού.

Άρθρο 2

Πρότυπα αναφοράς και προδιαγραφές για τη διαλειτουργικότητα μεταξύ εγκεκριμένων ηλεκτρονικών υπηρεσιών συστημένης παράδοσης

Τα πρότυπα αναφοράς και οι προδιαγραφές που αναφέρονται στο άρθρο 44 παράγραφος 2β του κανονισμού (ΕΕ) αριθ. 910/2014 καθορίζονται στο παράρτημα ΙΙ του παρόντος κανονισμού.

Άρθρο 3

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 Ι

Κατάλογος προτύπων αναφοράς και προδιαγραφών που αναφέρονται στο άρθρο 1

Ισχύει το πρότυπο ETSI EN 319 521 V1.1.1 (2019-02) («ETSI EN 319 521») με τις ακόλουθες προσαρμογές:

1. Όσον αφορά το ETSI EN 319 521

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 EN 319 411-1 V1.5.1 (2025-04) «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά· Μέρος 1: Γενικές απαιτήσεις».

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Ηλεκτρονικές υπηρεσίες συστημένης παράδοσης· Μέρος 1: Πλαίσιο και αρχιτεκτονική».

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) «Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Ηλεκτρονικές υπηρεσίες συστημένης παράδοσης· Μέρος 2: Σημασιολογικό περιεχόμενο».

— [5] 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]).

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

— [7] 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).

— [8] 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.

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

2) 3.1 Όροι

— προηγμένη ηλεκτρονική σφραγίδα: όπως ορίζεται στον κανονισμό (ΕΕ) αριθ. 910/2014 [i.1].

— προηγμένη ηλεκτρονική υπογραφή: όπως ορίζεται στον κανονισμό (ΕΕ) αριθ. 910/2014 [i.1].

— εγκεκριμένη ηλεκτρονική σφραγίδα: όπως ορίζεται στον κανονισμό (ΕΕ) αριθ. 910/2014 [i.1].

— εγκεκριμένη ηλεκτρονική υπογραφή: όπως ορίζεται στον κανονισμό (ΕΕ) αριθ. 910/2014 [i.1].

— 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.

([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.

3) 5.1.1 Κοινές διατάξεις

— REQ-ERDS-5.1.1-01 Η ηλεκτρονική υπηρεσία συστημένης παράδοσης (στο εξής: ERDS) διασφαλίζει ότι η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα του περιεχομένου των χρηστών διασφαλίζονται επαρκώς κατά τη διαχείρισή του από την ERDS, χάρη στην επιλογή κατάλληλων κρυπτογραφικών τεχνικών ακεραιότητας και εμπιστευτικότητας που συμμορφώνονται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα συνεργασίας για την κυβερνοασφάλεια και δημοσιεύει ο ENISA [5].

4) 5.2.1.1 Γενικά

— REQ-QERDS-5.2.1.1-01 Ο εγκεκριμένος πάροχος ηλεκτρονικών υπηρεσιών συστημένης παράδοσης (στο εξής: QERDSP) επαληθεύει με πολύ υψηλό επίπεδο εμπιστοσύνης την ταυτότητα του αποδέκτη είτε άμεσα είτε βασιζόμενος σε τρίτο μέρος και χρησιμοποιώντας ένα από τα ακόλουθα μέσα ή συνδυασμό αυτών, κατά περίπτωση:

α) με φυσική παρουσία του φυσικού προσώπου ή εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου, με κατάλληλα αποδεικτικά στοιχεία και διαδικασίες, σύμφωνα με το εθνικό δίκαιο·

β) εξ αποστάσεως, με τη χρήση συστήματος ηλεκτρονικής ταυτοποίησης, το οποίο πληροί τις απαιτήσεις που ορίζονται στο άρθρο 8 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1] όσον αφορά το «υψηλό» επίπεδο διασφάλισης, ή μέσω του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας·

γ) μέσω πιστοποιητικού εγκεκριμένης ηλεκτρονικής υπογραφής ή εγκεκριμένης ηλεκτρονικής σφραγίδας·

δ) με τη χρήση άλλων μεθόδων ταυτοποίησης, οι οποίες διασφαλίζουν ότι το φυσικό πρόσωπο ή ο εξουσιοδοτημένος εκπρόσωπος του νομικού προσώπου μπορεί να ταυτοποιηθεί με πολύ υψηλό επίπεδο εμπιστοσύνης. Η διασφάλιση ότι η εν λόγω ταυτοποίηση πραγματοποιείται με πολύ υψηλό επίπεδο εμπιστοσύνης επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης.

— REQ-QERDS-5.2.1.1-01A Ο QERDSP επαληθεύει την ταυτότητα του αποστολέα με κατάλληλα μέσα, είτε άμεσα είτε βασιζόμενος σε τρίτο μέρος, με βάση μία από τις ακόλουθες μεθόδους ή συνδυασμό αυτών:

α) με φυσική παρουσία του φυσικού προσώπου ή εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου, με κατάλληλα αποδεικτικά στοιχεία και διαδικασίες, σύμφωνα με το εθνικό δίκαιο·

β) εξ αποστάσεως, μέσω του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας ή κοινοποιημένου συστήματος ηλεκτρονικής ταυτοποίησης που πληροί τις απαιτήσεις που ορίζονται στο άρθρο 8 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1] όσον αφορά το «βασικό» επίπεδο διασφάλισης, υπό την προϋπόθεση ότι αυτό έχει εκδοθεί βάσει προηγούμενης φυσικής παρουσίας του φυσικού προσώπου ή εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου·

γ) μέσω πιστοποιητικού προηγμένης ηλεκτρονικής υπογραφής ή προηγμένης ηλεκτρονικής σφραγίδας, υπό την προϋπόθεση ότι το πιστοποιητικό έχει εκδοθεί για το φυσικό πρόσωπο ή για εξουσιοδοτημένο εκπρόσωπο του νομικού προσώπου βάσει της κανονικοποιημένης πολιτικής πιστοποιητικών (στο εξής: NCP), όπως ορίζεται στο ETSI EN 319 411-1 [2]· ή

δ) με τη χρήση άλλων μεθόδων ταυτοποίησης, οι οποίες διασφαλίζουν ότι το φυσικό πρόσωπο ή ο εξουσιοδοτημένος εκπρόσωπος του νομικού προσώπου μπορεί να ταυτοποιηθεί με πολύ υψηλό επίπεδο εμπιστοσύνης. Η διασφάλιση ότι η εν λόγω ταυτοποίηση πραγματοποιείται με υψηλό επίπεδο εμπιστοσύνης επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης.

— ΣΗΜΕΙΩΣΗ Το τρίτο μέρος που επαληθεύει την ταυτότητα του αποστολέα και του αποδέκτη μπορεί να είναι άλλος QERDSP, εάν ο αποστολέας και ο αποδέκτης είναι εγγεγραμμένοι σε διαφορετικούς QERDSP.

5) 5.2.1.2 Ταυτοποίηση αποδέκτη και παράδοση του περιεχομένου χρήστη

— REQ-QERDS-5.2.1.2-03 Εάν η ταυτοποίηση του αποδέκτη βασίζεται σε εσωτερική διαδικασία στο πλαίσιο της εγκεκριμένης ηλεκτρονικής υπηρεσίας συστημένης παράδοσης (στο εξής: QERDS), ο QERDSP διεξάγει ολόκληρη τη διαδικασία σε ασφαλές και ελεγχόμενο περιβάλλον.

6) 5.2.2 Διατάξεις για την ενωσιακή επαλήθευση ταυτότητας στο πλαίσιο της QERDS

— REQ-QERDS-5.2.2-03 [ΥΠΟ ΟΡΟΥΣ] Όταν ο QERDSP δεσμεύει σύστημα επαλήθευσης της ταυτότητας ενός αποστολέα που επαληθεύεται σύμφωνα με το σημείο 5.2.1, το εν λόγω σύστημα είναι ένα από τα ακόλουθα:

α) μηχανισμοί επαλήθευσης ταυτότητας δύο παραγόντων·

β) ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας ή κοινοποιημένο σύστημα ηλεκτρονικής ταυτοποίησης που πληροί τις απαιτήσεις του άρθρου 8 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1] όσον αφορά το «υψηλό» ή «βασικό» επίπεδο διασφάλισης·

γ) αμοιβαία επαλήθευση ασφάλειας επιπέδου μεταφοράς (στο εξής: TLS), η οποία περιλαμβάνει το πιστοποιητικό που εκδίδεται για τον αποστολέα βάσει της NCP, όπως ορίζεται στο ETSI EN 319 411-1 [2]·

δ) ψηφιακή υπογραφή υποστηριζόμενη από πιστοποιητικό που έχει εκδοθεί στο πλαίσιο της NCP, όπως ορίζεται στο ETSI EN 319 411-1 [2]·

ε) άλλο σύστημα που εξασφαλίζει την επαλήθευση της ταυτότητας του ταυτοποιημένου αποστολέα. Η συμμόρφωση της σύνδεσης επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης. Παράδειγμα: Αυτό μπορεί να περιλαμβάνει τη χρήση ενός από τα ανωτέρω συστήματα που αναφέρονται στα στοιχεία α), β) και δ) για την καταχώριση πιστοποιητικού πελάτη TLS με σκοπό την αυτοματοποιημένη αποστολή μέσω αμοιβαίου TLS, ή για την καταχώριση πιστοποιητικού ψηφιακής σφραγίδας που χρησιμοποιείται για τη σφράγιση βεβαιώσεων επαλήθευσης ταυτότητας στο πλαίσιο της ERDS. Μπορούν επίσης να εφαρμοστούν και άλλοι μηχανισμοί στο πλαίσιο των οποίων οι ταυτοποιημένοι αποστολείς χρησιμοποιούν εξουσιοδοτημένες υπηρεσίες τρίτων.

— REQ-QERDS-5.2.2-03A [ΥΠΟ ΟΡΟΥΣ] Όταν ο QERDSP δεσμεύει σύστημα επαλήθευσης της ταυτότητας ενός παραλήπτη που επαληθεύεται σύμφωνα με το σημείο 5.2.1, το εν λόγω σύστημα είναι ένα από τα ακόλουθα, υπό την προϋπόθεση ότι το σύστημα, ή τυχόν συνδυασμός συστημάτων, διασφαλίζει πολύ υψηλό επίπεδο εμπιστοσύνης όσον αφορά την ταυτότητα του επαληθευμένου αποδέκτη:

α) μηχανισμός επαλήθευσης ταυτότητας πολλαπλών παραγόντων·

β) ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας ή κοινοποιημένο σύστημα ηλεκτρονικής ταυτοποίησης που πληροί τις απαιτήσεις του άρθρου 8 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1] όσον αφορά το «υψηλό» ή «βασικό» επίπεδο διασφάλισης·

γ) πιστοποιητικό εγκεκριμένης ηλεκτρονικής υπογραφής ή εγκεκριμένης ηλεκτρονικής σφραγίδας·

δ) άλλο σύστημα που εξασφαλίζει την επαλήθευση της ταυτότητας του ταυτοποιημένου αποδέκτη. Η συμμόρφωση της σύνδεσης επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης. Παράδειγμα: Αυτό μπορεί να περιλαμβάνει τη χρήση ενός από τα ανωτέρω συστήματα που αναφέρονται στα στοιχεία α) έως γ) για την καταχώριση πιστοποιητικού πελάτη TLS με σκοπό την αυτοματοποιημένη αποστολή μέσω αμοιβαίου TLS, ή για την καταχώριση πιστοποιητικού ψηφιακής σφραγίδας που χρησιμοποιείται για τη σφράγιση βεβαιώσεων επαλήθευσης ταυτότητας στο πλαίσιο της ERDS. Μπορούν επίσης να εφαρμοστούν και άλλοι μηχανισμοί στο πλαίσιο των οποίων οι ταυτοποιημένοι αποστολείς χρησιμοποιούν εξουσιοδοτημένες υπηρεσίες τρίτων.

— REQ-QERDS-5.2.2-04 [ΥΠΟ ΟΡΟΥΣ] Εάν ο αποστολέας συνδέεται με την QERDS μέσω ασφαλούς σύνδεσης που απαιτεί αμοιβαία επαλήθευση ταυτότητας μηχανής προς μηχανή μεταξύ του μηχανήματος του αποστολέα και του εξυπηρετητή της QERDS βάσει πιστοποιητικών που έχουν εκδοθεί σύμφωνα με την NCP, όπως ορίζεται στο ETSI EN 319 411-1 [2], μετά τη δημιουργία της εν λόγω ασφαλούς σύνδεσης, μπορούν να εφαρμοστούν μηχανισμοί επαλήθευσης ταυτότητας ενός παράγοντα για τη δεύτερη φάση επαλήθευσης της ταυτότητας του αποστολέα, εάν οι οργανωτικές διαδικασίες και τα μέτρα ασφάλειας που εφαρμόζονται διασφαλίζουν την εμπιστοσύνη όσον αφορά την επαλήθευση της ταυτότητας του αποστολέα.

7) 5.4.1 Κοινές διατάξεις

— REQ-ERDS-5.4.1-06 Η ERDS δημιουργεί και θέτει στη διάθεση των νόμιμων ενδιαφερόμενων μερών στοιχεία της ERDS που αφορούν συμβάντα της ηλεκτρονικής συστημένης παράδοσης, όπως ορίζονται στο σημείο 6 του ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 Ο ERDSP αρχειοθετεί τα αποδεικτικά στοιχεία και/ή συνόψεις των αποδεικτικών στοιχείων για κάθε αποδεικτικό στοιχείο που έχει εκδώσει.

— REQ-ERDS-5.4.1-08 Τα αποδεικτικά στοιχεία της ERDS που δημιουργούνται από την ERDS συμμορφώνονται με τη σημασιολογία των αποδεικτικών στοιχείων που ορίζεται στο σημείο 8 του ETSI EN 319 522-2 [4].

8) 7.2.1 Κοινές διατάξεις

— REQ-ERDS-7.2.1-02 Τα μέλη του προσωπικού του ERDSP 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.

— REQ-ERDS-7.2,1-03 Η συμμόρφωση με η REQ-ERDS-7.2,1-02 περιλαμβάνει τακτικές ενημερώσεις (τουλάχιστον κάθε 12 μήνες) σχετικά με τις νέες απειλές και τις τρέχουσες πρακτικές ασφάλειας.

9) 7.3.2 Διαχείριση μέσων

— REQ-ERDS-7.3.1-02 Ισχύουν όλες οι απαιτήσεις του ETSI EN 319 401 [1], σημείο 7.3.3.

10) 7.5 Κρυπτογραφικοί έλεγχοι

— REQ-ERDS-7.5-01A Η ERDS επιλέγει και χρησιμοποιεί κατάλληλες κρυπτογραφικές τεχνικές σύμφωνα με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα συνεργασίας για την κυβερνοασφάλεια και δημοσιεύει ο ENISA [5].

— REQ-ERDSP-7.5-03 Το ιδιωτικό κλειδί υπογραφής της ERDS 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 [6] 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) [7][8], και πιστοποιημένο κατά το πρότυπο EAL 4 ή ανώτερο· ή

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

11) 7.8 Ασφάλεια δικτύου

— REQ-ERDSP-7.8-04 Ο ERDSP χρησιμοποιεί προηγμένα πρωτόκολλα και αλγόριθμους για την κρυπτογράφηση σε επίπεδο μεταφοράς σύμφωνα με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο ENISA [5].

— REQ-ERDSP-7.8-06 Η σάρωση τρωτών σημείων που απαιτείται από το REQ-7.8-13 του ETSI EN 319 401 [1] εκτελείται τουλάχιστον μία φορά ανά τρίμηνο.

— REQ-ERDSP-7.8-07 Η δοκιμή παρείσδυσης που απαιτείται από τη REQ-7.8-17X του ETSI EN 319 401 [1] εκτελείται τουλάχιστον μία φορά ετησίως.

— REQ-ERDSP-7.8-08 Τα τείχη προστασίας διαμορφώνονται έτσι ώστε να αποτρέπονται όλα τα πρωτόκολλα και οι προσβάσεις που δεν απαιτούνται για τη λειτουργία του παρόχου υπηρεσιών εμπιστοσύνης.

12) 7.12 Τερματισμός του ERDSP και σχέδια τερματισμού της ERDS

— REQ-ERDS-7.12-03 Το σχέδιο τερματισμού του ERDSP 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].

13) 7.14 Αλυσίδα εφοδιασμού

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

ΠΑΡΑΡΤΗΜΑ II

Κατάλογος προτύπων αναφοράς και προδιαγραφών που αναφέρονται στο άρθρο 2

Ισχύουν τα πρότυπα ETSI EN 319 522-1 V1.2.1 (2024-01) («ETSI EN 319 522-1»), ETSI EN 319 522-2 V1.2.1 (2024-01) («ETSI EN 319 522-2»), ETSI EN 319 522-3 V1.2.1 (2024-01) («ETSI EN 319 522-3»), ETSI EN 319 522-4-1 V1.2.1 (2019-01) («ETSI EN 319 522-4-1»), ETSI EN 319 522-4-2 V1.1.1 (2018-09) («ETSI EN 319 522-4-2») και ETSI EN 319 522-4-3 V1.1.1 (2018-09) («ETSI EN 319 522-4-3»).