Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2024/2981

4.12.2024

# ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/2981 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

**της 28ης Νοεμβρίου 2024**

**για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την πιστοποίηση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας**

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 5γ παράγραφος 6,

Εκτιμώντας τα ακόλουθα:

(1) Σύμφωνα με το άρθρο 5γ του κανονισμού (ΕΕ) αριθ. 910/2014, η πιστοποίηση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας (στο εξής: «πορτοφόλια»), πρέπει να πραγματοποιείται σύμφωνα με λειτουργικές απαιτήσεις, απαιτήσεις κυβερνοασφάλειας και απαιτήσεις προστασίας των δεδομένων, ώστε να διασφαλίζεται υψηλό επίπεδο ασφάλειας και εμπιστοσύνης στα πορτοφόλια. Οι εν λόγω απαιτήσεις πιστοποίησης πρέπει να εναρμονιστούν σε όλα τα κράτη μέλη προκειμένου να αποτραπεί ο κατακερματισμός της αγοράς και να δημιουργηθεί ένα ισχυρό πλαίσιο.

(2) Στις δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του παρόντος κανονισμού εφαρμόζεται ο κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]) και, κατά περίπτωση, η οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]).

(3) Η Επιτροπή αξιολογεί τακτικά νέες τεχνολογίες, πρακτικές, πρότυπα ή τεχνικές προδιαγραφές. Προκειμένου να διασφαλιστεί το υψηλότερο δυνατό επίπεδο εναρμόνισης μεταξύ των κρατών μελών για την ανάπτυξη και την πιστοποίηση των πορτοφολιών, οι τεχνικές προδιαγραφές που ορίζονται στον παρόντα κανονισμό βασίζονται στις εργασίες που πραγματοποιήθηκαν με βάση τη σύσταση (ΕΕ) 2021/946 της Επιτροπής, της 3ης Ιουνίου 2021, σχετικά με κοινή εργαλειοθήκη της Ένωσης για μια συντονισμένη προσέγγιση όσον αφορά το ευρωπαϊκό πλαίσιο για την ψηφιακή ταυτότητα ([4]), και ιδίως την αρχιτεκτονική και το πλαίσιο αναφοράς που αποτελεί μέρος του. Σύμφωνα με την αιτιολογική σκέψη 75 του κανονισμού (ΕΕ) 2024/1183 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([5]), η Επιτροπή θα πρέπει να επανεξετάζει και, εάν χρειάζεται, να επικαιροποιεί τον παρόντα εκτελεστικό κανονισμό, ώστε να συμβαδίζει με τις παγκόσμιες εξελίξεις, την αρχιτεκτονική και το πλαίσιο αναφοράς και να ακολουθούνται οι βέλτιστες πρακτικές στην εσωτερική αγορά.

(4) Προκειμένου να πιστοποιείται η συμμόρφωση με τις απαιτήσεις κυβερνοασφάλειας που περιλαμβάνονται στο πλαίσιο πιστοποίησης, η πιστοποίηση υλοποιήσεων πορτοφολιών θα πρέπει να αναφέρεται, εφόσον υπάρχουν και κατά περίπτωση, στα ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας που θεσπίζονται σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. ([6]) Ελλείψει τέτοιων σχημάτων, ή όταν καλύπτουν εν μέρει τις απαιτήσεις κυβερνοασφάλειας, ο παρών κανονισμός καθορίζει τις γενικές απαιτήσεις που ισχύουν για τα εθνικά σχήματα πιστοποίησης, οι οποίες καλύπτουν τις λειτουργικές απαιτήσεις, τις απαιτήσεις κυβερνοασφάλειας και τις απαιτήσεις προστασίας των δεδομένων.

([1]) ΕΕ L 257 της 28.8.2014, σ. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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).

([3]) 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).

([4]) ΕΕ L 210 της 14.6.2021, σ. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([5]) 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 της 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([6]) Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Σύμφωνα με το άρθρο 5α παράγραφος 11 του κανονισμού (ΕΕ) αριθ. 910/2014, τα πορτοφόλια πρέπει να πιστοποιούνται έναντι υψηλού επιπέδου διασφάλισης, όπως ορίζεται στον κανονισμό (ΕΕ) αριθ. 910/2014, καθώς και στον εκτελεστικό κανονισμό (ΕΕ) 2015/1502 της Επιτροπής ([7]). Αυτό το επίπεδο διασφάλισης πρέπει να επιτυγχάνεται από τη συνολική υλοποίηση πορτοφολιού. Σύμφωνα με τον παρόντα κανονισμό, ορισμένα συστατικά στοιχεία της υλοποίησης πορτοφολιού μπορούν να πιστοποιούνται σε χαμηλότερο επίπεδο διασφάλισης, υπό την προϋπόθεση ότι αυτό αιτιολογείται δεόντως και με την επιφύλαξη της επίτευξης υψηλού επιπέδου διασφάλισης από τη συνολική υλοποίηση.

(6) Όλα τα εθνικά σχήματα πιστοποίησης θα πρέπει να ορίζουν έναν ιδιοκτήτη σχήματος ο οποίος θα είναι υπεύθυνος για την ανάπτυξη και τη συντήρηση του σχήματος πιστοποίησης. Ο ιδιοκτήτης του σχήματος μπορεί να είναι οργανισμός αξιολόγησης της συμμόρφωσης, κυβερνητικός φορέας ή αρχή, εμπορική ένωση, ομάδα οργανισμών αξιολόγησης της συμμόρφωσης ή οποιοσδήποτε αρμόδιος φορέας και μπορεί να διαφέρει από τον φορέα που διαχειρίζεται το εθνικό σχήμα πιστοποίησης.

(7) Το αντικείμενο της πιστοποίησης θα πρέπει να περιλαμβάνει τα στοιχεία λογισμικού της υλοποίησης πορτοφολιού, όπως τα στιγμιότυπα πορτοφολιού. Η ασφαλής κρυπτογραφική εφαρμογή πορτοφολιού (στο εξής: «WSCA»), η ασφαλής κρυπτογραφική διάταξη πορτοφολιού («WSCD») και οι πλατφόρμες στις οποίες εκτελούνται τα εν λόγω συστατικά στοιχεία λογισμικού, ενώ αποτελούν μέρος του επιχειρησιακού περιβάλλοντος, θα πρέπει να περιλαμβάνονται στο αντικείμενο της πιστοποίησης μόνο όταν παρέχονται από την υλοποίηση πορτοφολιού. Σε άλλες περιπτώσεις, και ιδίως όταν οι εν λόγω διατάξεις και πλατφόρμες παρέχονται από τελικούς χρήστες, οι πάροχοι θα πρέπει να καθορίζουν παραδοχές σχετικά με το λειτουργικό περιβάλλον της υλοποίησης πορτοφολιού, συμπεριλαμβανομένων των εν λόγω διατάξεων και πλατφορμών, και να εφαρμόζουν μέτρα για να επιβεβαιώνουν ότι οι παραδοχές αυτές επαληθεύονται στην πράξη. Προκειμένου να διασφαλιστεί η προστασία των κρίσιμων περιουσιακών στοιχείων μέσω του υλισμικού και του λογισμικού του συστήματος που χρησιμοποιείται για τη διαχείριση και την προστασία κρυπτογραφικών κλειδιών που δημιουργούνται, αποθηκεύονται ή υποβάλλονται σε επεξεργασία από την WSCD, η WSCD πρέπει να πληροί υψηλά πρότυπα πιστοποίησης, μέσω αξιολόγησης κατά EAL4 και μέσω της προηγμένης μεθοδολογικής ανάλυσης τρωτότητας, συγκρίσιμης με το πρότυπο AVA_VAN.5., όπως αποτυπώνονται σε διεθνή πρότυπα, π.χ. στην αξιολόγηση κοινών κριτηρίων («EUCC»), που θεσπίστηκαν με τον εκτελεστικό κανονισμό (ΕΕ) 2024/482 της Επιτροπής ([8]). Τα εν λόγω πρότυπα πιστοποίησης θα πρέπει να χρησιμοποιούνται το αργότερο όταν η πιστοποίηση της συμμόρφωσης των πορτοφολιών πραγματοποιείται σύμφωνα με ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας το οποίο έχει υιοθετηθεί βάσει του κανονισμού (ΕΕ) 2019/881.

(8) Τα πλήρως κινητά, ασφαλή και εύχρηστα πορτοφόλια, υποστηρίζονται από τη διαθεσιμότητα τυποποιημένων και πιστοποιημένων υλοποιήσεων ανθεκτικών στην παραποίηση, όπως ενσωματωμένα ασφαλή στοιχεία, εξωτερικές διατάξεις όπως «έξυπνες κάρτες», ή ενσωματωμένες πλατφόρμες SIM σε κινητές συσκευές. Είναι σημαντικό να διασφαλιστεί η έγκαιρη πρόσβαση σε ενσωματωμένα ασφαλή στοιχεία για τα εθνικά μέσα και πορτοφόλια ηλεκτρονικής ταυτοποίησης και να συντονιστούν οι προσπάθειες των κρατών μελών στον τομέα αυτό. Ως εκ τούτου, η ομάδα συνεργασίας για την ευρωπαϊκή ψηφιακή ταυτότητα που συστάθηκε σύμφωνα με το άρθρο 46ε παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014 (στο εξής: «ομάδα συνεργασίας»), θα πρέπει να συστήσει ειδική υποομάδα για τον σκοπό αυτό. Κατόπιν διαβούλευσης με τα σχετικά ενδιαφερόμενα μέρη, η εν λόγω υποομάδα θα πρέπει να συμφωνήσει επί κοινού χάρτη πορείας για την πρόσβαση σε ενσωματωμένα ασφαλή στοιχεία που θα εξετάσει η Επιτροπή για την έκθεση επανεξέτασης του κανονισμού (ΕΕ) αριθ. 910/2014. Προκειμένου να διευκολυνθεί η υιοθέτηση του πορτοφολιού σε εθνικό επίπεδο, η Επιτροπή θα πρέπει, επιπλέον, σε συνεργασία με τα κράτη μέλη, να αναπτύξει και να επικαιροποιεί συνεχώς εγχειρίδιο για τις περιπτώσεις χρήσης ως μέρος του πλαισίου αρχιτεκτονικής και αναφοράς.

(9) Το αντικείμενο της πιστοποίησης εθνικών σχημάτων πιστοποίησης θα πρέπει επίσης να περιλαμβάνει τις διαδικασίες που χρησιμοποιούνται για την παροχή και τη λειτουργία της υλοποίησης πορτοφολιού, ακόμα και αν ο καθορισμός ή η εκτέλεση των εν λόγω διαδικασιών ανατίθεται υπεργολαβικά σε τρίτους. Προκειμένου να αποδειχθεί ότι οι διαδικασίες πληρούν τις απαιτήσεις των σχημάτων, επιτρέπεται να χρησιμοποιούνται ως αποδεικτικά στοιχεία πληροφορίες διασφάλισης, υπό την προϋπόθεση ότι χρησιμοποιείται ανάλυση εξάρτησης για να διαπιστωθεί αν οι πληροφορίες διασφάλισης είναι επαρκείς. Οι πληροφορίες διασφάλισης παρέχονται σε πολλές διαφορετικές μορφές, όπως εκθέσεις και πιστοποιητικά συμμόρφωσης, τα οποία μπορεί να είναι ιδιωτικά, εθνικά, ευρωπαϊκά ή διεθνή, βασισμένα σε πρότυπα ή τεχνικές προδιαγραφές. Στόχος της ανάλυσης εξάρτησης είναι η αξιολόγηση της ποιότητας των διαθέσιμων πληροφοριών διασφάλισης σχετικά με τα συστατικά στοιχεία ενός πορτοφολιού.

([7]) Εκτελεστικός κανονισμός (ΕΕ) 2015/1502 της Επιτροπής, της 8ης Σεπτεμβρίου 2015, σχετικά με τη θέσπιση ελάχιστων τεχνικών προδιαγραφών και διαδικασιών για τα επίπεδα διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης σύμφωνα με το άρθρο 8 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά, ΕΕ L 235 της 9.9.2015, σ. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) Εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής, 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) (ΕΕ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Σύμφωνα με τις διαδικασίες που θεσπίζονται για τον σκοπό αυτό, η ομάδα συνεργασίας θα πρέπει να είναι σε θέση να διατυπώνει γνώμες και συστάσεις σχετικά με τα σχέδια εθνικών σχημάτων πιστοποίησης που της υποβάλλονται. Τα εν λόγω εθνικά σχήματα πιστοποίησης θα πρέπει να αφορούν ειδικά την αρχιτεκτονική του πορτοφολιού και θα πρέπει να υπάρχουν ειδικά προφίλ για κάθε συγκεκριμένη αρχιτεκτονική που υποστηρίζεται.

(11) Προκειμένου να διασφαλιστεί κοινή αντίληψη και εναρμονισμένη προσέγγιση όσον αφορά την αξιολόγηση των πλέον κρίσιμων κινδύνων που ενδέχεται να επηρεάσουν την παροχή και τη λειτουργία των πορτοφολιών, θα πρέπει να καταρτιστεί μητρώο κινδύνων και απειλών το οποίο θα πρέπει να λαμβάνεται υπόψη κατά τον σχεδιασμό υλοποιήσεων πορτοφολιού ανεξάρτητα από τη συγκεκριμένη αρχιτεκτονική τους. Οι στόχοι κυβερνοασφάλειας που περιγράφονται στον κανονισμό (ΕΕ) αριθ. 910/2014, όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα της υλοποίησης πορτοφολιού, καθώς και η προστασία της ιδιωτικής ζωής των χρηστών και των δεδομένων, θα πρέπει να λαμβάνονται υπόψη κατά τον προσδιορισμό των κινδύνων που θα πρέπει να περιλαμβάνονται στο μητρώο. Η δέουσα συνεκτίμηση των κινδύνων και των απειλών που περιλαμβάνονται στο εν λόγω μητρώο κινδύνων θα πρέπει να αποτελεί μέρος των απαιτήσεων των εθνικών σχημάτων πιστοποίησης. Για να συμβαδίζει με το συνεχώς εξελισσόμενο τοπίο των απειλών, το μητρώο κινδύνων θα πρέπει να τηρείται και να επικαιροποιείται τακτικά, σε συνεργασία με την ομάδα συνεργασίας.

(12) Κατά τη δημιουργία των σχημάτων πιστοποίησής τους, οι ιδιοκτήτες σχημάτων θα πρέπει να διενεργούν εκτίμηση κινδύνου για τη βελτίωση και τη συμπλήρωση των κινδύνων και των απειλών που περιλαμβάνονται στο μητρώο με κινδύνους και απειλές που αφορούν ειδικά την αρχιτεκτονική ή την εφαρμογή της υλοποίησης πορτοφολιού. Η εκτίμηση κινδύνου θα πρέπει να εξετάζει τον τρόπο με τον οποίο μπορούν να αντιμετωπιστούν κατάλληλα οι ισχύοντες κίνδυνοι και απειλές. Οι πάροχοι πορτοφολιών θα πρέπει να συμπληρώνουν την εκτίμηση κινδύνου του σχήματος για τον εντοπισμό τυχόν κινδύνων και απειλών που αφορούν ειδικά την εφαρμογή τους και να προτείνουν κατάλληλα μέτρα αντιμετώπισης προς αξιολόγηση από τον φορέα πιστοποίησης.

(13) Για να αποδειχθεί ότι μια αρχιτεκτονική υλοποίησης πορτοφολιού πληροί τις εφαρμοστέες απαιτήσεις ασφάλειας, κάθε ειδικό ανά αρχιτεκτονική σχήμα ή προφίλ θα πρέπει να περιέχει τουλάχιστον περιγραφή της αρχιτεκτονικής της υλοποίησης πορτοφολιού, κατάλογο των απαιτήσεων ασφάλειας που ισχύουν για την αρχιτεκτονική της υλοποίησης πορτοφολιού, σχέδιο αξιολόγησης για να επιβεβαιωθεί ότι μια υλοποίηση πορτοφολιού με βάση τη συγκεκριμένη αρχιτεκτονική πληροί τις εν λόγω απαιτήσεις, καθώς και εκτίμηση κινδύνου. Τα εθνικά σχήματα πιστοποίησης θα πρέπει να απαιτούν από τους παρόχους πορτοφολιών να αποδεικνύουν τον τρόπο με τον οποίο ο σχεδιασμός της υλοποίησης πορτοφολιού που παρέχουν αντιστοιχεί στην αρχιτεκτονική αναφοράς και περιγράφει λεπτομερώς τους ελέγχους ασφάλειας και τα σχέδια επικύρωσης για τη συγκεκριμένη υλοποίηση πορτοφολιού. Τα εθνικά σχήματα πιστοποίησης θα πρέπει επίσης να καθορίζουν μια δραστηριότητα αξιολόγησης της συμμόρφωσης προκειμένου να επαληθεύεται ότι ο σχεδιασμός του πορτοφολιού αντικατοπτρίζει ορθά την αρχιτεκτονική αναφοράς του επιλεγμένου προφίλ. Τα εθνικά σχήματα πιστοποίησης θα πρέπει να πληρούν τις απαιτήσεις που ορίζονται στο άρθρο 51 του κανονισμού (ΕΕ) 2019/881, πλην των στοιχείων ε) και στ) που αφορούν την καταγραφή.

(14) Όσον αφορά την πιστοποίηση προϊόντων, θα πρέπει να επιτρέπεται η χρήση πιστοποιητικών συμμόρφωσης που εκδίδονται στο πλαίσιο του ενωσιακού σχήματος πιστοποίησης της κυβερνοασφάλειας (στο εξής: «EUCC»), και πιστοποιητικών συμμόρφωσης που εκδίδονται βάσει εθνικών σχημάτων πιστοποίησης στο πλαίσιο της συμφωνίας αμοιβαίας αναγνώρισης της Ομάδας Ανώτερων Υπαλλήλων για την Ασφάλεια των Συστημάτων Πληροφοριών (SOG-IS). Επιπλέον, θα πρέπει να επιτρέπεται η χρήση άλλων εθνικών σχημάτων πιστοποίησης για λιγότερο ευαίσθητα συστατικά στοιχεία προϊόντων, όπως εκείνα που θεσπίζονται σύμφωνα με το πρότυπο CEN EN 17640 για τη μεθοδολογία αξιολόγησης της κυβερνοασφάλειας σε καθορισμένους χρόνους.

(15) Θα πρέπει να χρησιμοποιείται το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ (στο εξής: σήμα εμπιστοσύνης) για να επισημαίνεται με σαφή, απλό και αναγνωρίσιμο τρόπο ότι ένα πορτοφόλι έχει παρασχεθεί σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014. Ως εκ τούτου, θα πρέπει να θεωρείται σήμα συμμόρφωσης για μια υλοποίηση πορτοφολιού που έχει πιστοποιηθεί στο πλαίσιο εθνικών σχημάτων πιστοποίησης. Τα εθνικά σχήματα πιστοποίησης δεν θα πρέπει να καθορίζουν άλλα σήματα συμμόρφωσης.

(16) Προκειμένου να αποθαρρύνεται η απάτη, τα εθνικά σχήματα πιστοποίησης θα πρέπει να καθορίζουν τα μέτρα που πρέπει να λαμβάνονται όταν ζητείται δολίως πιστοποίηση στο πλαίσιο του σχήματος.

(17) Για να διασφαλιστεί η αποτελεσματική διαχείριση των κοινοποιήσεων τρωτών σημείων, οι πάροχοι υλοποιήσεων πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχονται θα πρέπει να καθορίζουν και να εφαρμόζουν διαδικασίες για την αξιολόγηση της σοβαρότητας και του δυνητικού αντικτύπου των τρωτών σημείων. Τα εθνικά σχήματα πιστοποίησης θα πρέπει να καθορίζουν ένα κατώτατο όριο πάνω από το οποίο πρέπει να ενημερώνεται ο οργανισμός πιστοποίησης. Η εν λόγω υποχρέωση κοινοποίησης δεν θα πρέπει να θίγει τα κριτήρια που θεσπίζονται από τη νομοθεσία για την προστασία των δεδομένων και τις αρχές προστασίας δεδομένων των κρατών μελών για την κοινοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα. Θα μπορούσαν να δημιουργηθούν πιθανές συνέργειες μεταξύ της υποχρεωτικής κοινοποίησης παραβίασης ή έκθεσης σε κίνδυνο των υλοποιήσεων πορτοφολιού και της κοινοποίησης παραβιάσεων δεδομένων προσωπικού χαρακτήρα σύμφωνα με τον κανονισμό (ΕΕ) 2016/679. Η αξιολόγηση μιας έκθεσης ανάλυσης επιπτώσεων τρωτότητας από τον οργανισμό πιστοποίησης θα πρέπει να διενεργείται με την επιφύλαξη της αξιολόγησης μιας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων η οποία διενεργείται από αρχή προστασίας δεδομένων σύμφωνα με τα άρθρα 35 και 36 του κανονισμού (ΕΕ) 2016/679.

(18) Οι πάροχοι υλοποιήσεων πορτοφολιών και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτές παρέχονται θα πρέπει να κοινοποιούν στον ιδιοκτήτη του σχήματος τυχόν αιτιολογήσεις για εξαιρέσεις από την εκτίμηση τρωτότητας που απαιτείται για την αξιολόγηση των WSCD και WSCA, όπως ορίζεται στο παράρτημα IV.

(19) Η ακύρωση πιστοποιητικού συμμόρφωσης ενδέχεται να έχει σοβαρές συνέπειες, όπως ανάκληση όλων των εγκατεστημένων μονάδων πορτοφολιού. Ως εκ τούτου, οι οργανισμοί πιστοποίησης θα πρέπει να εξετάζουν το ενδεχόμενο ακύρωσης μόνο εάν ένα μη διορθωμένο τρωτό σημείο είναι πιθανό να επηρεάσει σημαντικά την αξιοπιστία της υλοποίησης πορτοφολιού ή την αξιοπιστία άλλης υλοποίησης πορτοφολιού.

(20) Θα πρέπει να θεσπιστεί ειδική διαδικασία για την επικαιροποίηση των εθνικών σχημάτων πιστοποίησης με σκοπό τη διαχείριση της μετάβασης μεταξύ διαδοχικών εκδόσεων των σχημάτων, ιδίως σε σχέση με τα μέτρα που πρέπει να λαμβάνει ο κάτοχος του πιστοποιητικού όσον αφορά τις επικείμενες αξιολογήσεις, τη συντήρηση, την επαναπιστοποίηση και τις ειδικές αξιολογήσεις.

(21) Για να διευκολυνθεί η διαφάνεια, οι πάροχοι πορτοφολιών θα πρέπει να ανταλλάσσουν δημόσια πληροφορίες ασφάλειας σχετικά με την υλοποίηση πορτοφολιού τους.

(22) Όταν τα εθνικά σχήματα πιστοποίησης βασίζονται σε πληροφορίες διασφάλισης από άλλα σχήματα ή πηγές πιστοποίησης, θα πρέπει να διενεργείται ανάλυση εξάρτησης ώστε να επαληθεύεται ότι η τεκμηρίωση διασφάλισης, για παράδειγμα εκθέσεις διασφάλισης και πιστοποιητικά συμμόρφωσης, είναι διαθέσιμη και επαρκής για την υλοποίηση πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται. Η βάση για την εν λόγω ανάλυση εξάρτησης θα πρέπει να είναι η εκτίμηση κινδύνου της υλοποίησης πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται. Η αξιολόγηση θα πρέπει να προσδιορίζει αν η τεκμηρίωση διασφάλισης που είναι διαθέσιμη για μια συγκεκριμένη υλοποίηση πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται επαρκεί για την παροχή διασφάλισης η οποία αντιστοιχεί στο στοχευμένο επίπεδο αξιολόγησης. Στο πλαίσιο της αξιολόγησης θα πρέπει επίσης να επικαιροποιείται η ανάλυση εξάρτησης ή να γίνεται πλήρης επαναξιολόγησή της, όπου είναι αναγκαίο.

(23) Οι οργανισμοί πιστοποίησης θα πρέπει να εκδίδουν πιστοποιητικά συμμόρφωσης στα εθνικά σχήματα πιστοποίησης, μαζί με δημόσια διαθέσιμη έκθεση πιστοποίησης, όπως αναφέρεται στο άρθρο 5δ παράγραφος 2 στοιχείο α) του κανονισμού (ΕΕ) αριθ. 910/2014. Η σχετική έκθεση αξιολόγησης της πιστοποίησης θα πρέπει να τίθεται στη διάθεση της ομάδας συνεργασίας.

(24) Τα εθνικά σχήματα πιστοποίησης θα πρέπει να καθορίζουν ετήσια αξιολόγηση εποπτείας ώστε να διασφαλίζεται ότι οι διαδικασίες σχετικά με τη διαχείριση και τη συντήρηση των πορτοφολιών λειτουργούν αποτελεσματικά, δηλαδή λειτουργούν όπως ορίζεται στις πολιτικές που καθορίζουν τις διαδικασίες. Η ανά διετία αξιολόγηση τρωτότητας αποτελεί απαίτηση που απορρέει από τον κανονισμό (ΕΕ) αριθ. 910/2014, ώστε να διασφαλίζεται ότι η υλοποίηση πορτοφολιού εξακολουθεί να καλύπτει κατάλληλα τους κινδύνους και τις απειλές κυβερνοασφάλειας που προσδιορίζονται στο μητρώο κινδύνων, συμπεριλαμβανομένης τυχόν εξέλιξης του τοπίου των απειλών. Οι έννοιες των αξιολογήσεων εποπτείας, των αξιολογήσεων επαναπιστοποίησης και των ειδικών αξιολογήσεων θα πρέπει να είναι σύμφωνες με το πρότυπο EN ISO/IEC 17021-1: 2015.

(25) Ο κύκλος πιστοποίησης ολοκληρώνεται με τη λήξη του πιστοποιητικού συμμόρφωσης ή με την έκδοση νέου πιστοποιητικού συμμόρφωσης μετά από επιτυχή αξιολόγηση επαναπιστοποίησης. Η αξιολόγηση επαναπιστοποίησης θα πρέπει να περιλαμβάνει αξιολόγηση όλων των συστατικών στοιχείων του αντικειμένου της πιστοποίησης, συμπεριλαμβανομένης αξιολόγησης της αποτελεσματικότητας και, κατά περίπτωση, αξιολόγησης τρωτότητας. Κατά την επαναπιστοποίηση, θα πρέπει να είναι δυνατή η επαναχρησιμοποίηση των αποτελεσμάτων προηγούμενων αξιολογήσεων για συστατικά στοιχεία που δεν έχουν αλλάξει.

(26) Όταν θεσπίζεται ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας, τα εθνικά σχήματα πιστοποίησης με το ίδιο πεδίο εφαρμογής θα πρέπει να παύουν να εκδίδουν πιστοποιήσεις μετά από καθορισμένη μεταβατική περίοδο, όπως αναφέρεται στο άρθρο 57 παράγραφος 1 του κανονισμού (ΕΕ) 2019/881.

(27) Τα εθνικά σχήματα πιστοποίησης θα πρέπει να βασίζονται σε υφιστάμενα πλαίσια και να επαναχρησιμοποιούν αποδεικτικά στοιχεία κατά περίπτωση, προκειμένου να διασφαλίζεται η εναρμόνιση και η διαλειτουργικότητα. Τα κράτη μέλη μπορούν να συνάπτουν συμφωνίες για τη διασυνοριακή επαναχρησιμοποίηση σχημάτων πιστοποίησης ή μερών αυτών. Η Ευρωπαϊκή Επιτροπή και ο ENISA θα πρέπει, σε συνεργασία με την ομάδα συνεργασίας, να στηρίζουν τα κράτη μέλη κατά την κατάρτιση και συντήρηση των εθνικών τους σχημάτων πιστοποίησης, διασφαλίζοντας την ανταλλαγή γνώσεων και βέλτιστων πρακτικών.

(28) Ζητήθηκε, σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9]), η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις 30 Σεπτεμβρίου 2024.

(29) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που αναφέρεται στο άρθρο 48 παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

ΚΕΦΑΛΑΙΟ I

**ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ**

*Άρθρο 1*

**Αντικείμενο και πεδίο εφαρμογής**

Ο παρών κανονισμός καθορίζει πρότυπα αναφοράς και θεσπίζει προδιαγραφές και διαδικασίες για τη δημιουργία ενός ισχυρού πλαισίου για την πιστοποίηση πορτοφολιών, το οποίο θα επικαιροποιείται σε τακτική βάση ώστε να συμβαδίζει με τις εξελίξεις στην τεχνολογία και στα πρότυπα και με τις εργασίες που διεξάγονται βάσει της σύστασης (ΕΕ) 2021/946 σχετικά με κοινή εργαλειοθήκη της Ένωσης για μια συντονισμένη προσέγγιση όσον αφορά ένα ευρωπαϊκό πλαίσιο για την ψηφιακή ταυτότητα, και ιδίως την αρχιτεκτονική και το πλαίσιο αναφοράς.

*Άρθρο 2*

**Ορισμοί**

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

1) «υλοποίηση πορτοφολιού»: συνδυασμός λογισμικού, υλισμικού, υπηρεσιών, ρυθμίσεων και διαμορφώσεων, συμπεριλαμβανομένων των στιγμιότυπων πορτοφολιού, μίας ή περισσότερων ασφαλών κρυπτογραφικών εφαρμογών πορτοφολιού και μίας ή περισσότερων ασφαλών κρυπτογραφικών διατάξεων πορτοφολιού·

2) «ιδιοκτήτης σχήματος»: οργανισμός που είναι υπεύθυνος για την ανάπτυξη και συντήρηση σχήματος πιστοποίησης·

3) «αντικείμενο πιστοποίησης»: προϊόντα, διαδικασίες και υπηρεσίες ή συνδυασμός αυτών, για τα οποία ισχύουν συγκεκριμένες απαιτήσεις·

4) «ασφαλής κρυπτογραφική εφαρμογή πορτοφολιού»: εφαρμογή που διαχειρίζεται κρίσιμα περιουσιακά στοιχεία μέσω της σύνδεσής της με τις κρυπτογραφικές και μη κρυπτογραφικές λειτουργίες που παρέχει η ασφαλής κρυπτογραφική διάταξη πορτοφολιού και μέσω της χρήσης αυτών·

5) «στιγμιότυπο πορτοφολιού»: η εφαρμογή όπως έχει εγκατασταθεί και έχει διαμορφωθεί σε διάταξη ή περιβάλλον χρήστη πορτοφολιού, η οποία αποτελεί μέρος μονάδας πορτοφολιού, και την οποία χρησιμοποιεί ο χρήστης πορτοφολιού για να αλληλεπιδρά με τη μονάδα πορτοφολιού·

([9]) 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).

6) «ασφαλής κρυπτογραφική διάταξη πορτοφολιού»: ανθεκτική στην παραβίαση διάταξη η οποία παρέχει περιβάλλον το οποίο συνδέεται και χρησιμοποιείται από την ασφαλή κρυπτογραφική εφαρμογή του πορτοφολιού για την προστασία κρίσιμων περιουσιακών στοιχείων και την παροχή κρυπτογραφικών λειτουργιών για την ασφαλή εκτέλεση κρίσιμων λειτουργιών·

7) «μητρώο κινδύνων»: αρχείο πληροφοριών σχετικών με τη διαδικασία πιστοποίησης για εντοπισθέντες κινδύνους·

8) «πάροχος πορτοφολιού»: φυσικό ή νομικό πρόσωπο το οποίο παρέχει υλοποιήσεις πορτοφολιού·

9) «οργανισμός πιστοποίησης»: τρίτος οργανισμός αξιολόγησης της συμμόρφωσης ο οποίος διαχειρίζεται σχήματα πιστοποίησης·

10) «μονάδα πορτοφολιού»: μοναδική διαμόρφωση μιας υλοποίησης πορτοφολιού που περιλαμβάνει στιγμιότυπα πορτοφολιού, ασφαλείς κρυπτογραφικές εφαρμογές πορτοφολιού και ασφαλείς κρυπτογραφικές διατάξεις πορτοφολιού που παρέχονται από έναν πάροχο πορτοφολιού σε μεμονωμένο χρήστη πορτοφολιού·

11) «κρίσιμα περιουσιακά στοιχεία»: περιουσιακά στοιχεία εντός μονάδας πορτοφολιού ή σχετιζόμενα με μονάδα πορτοφολιού, τα οποία είναι τόσο εξέχουσας σημασίας ώστε όταν τίθεται σε κίνδυνο η διαθεσιμότητα, η εμπιστευτικότητα ή η ακεραιότητά τους, αυτό μπορεί να έχει πολύ σοβαρές, ανεπανόρθωτες επιπτώσεις στην ικανότητα των ατόμων να βασίζονται στη μονάδα πορτοφολιού·

12) «χρήστης πορτοφολιού»: χρήστης που έχει τον έλεγχο της μονάδας πορτοφολιού·

13) «περιστατικό»: περιστατικό όπως ορίζεται στο άρθρο 6 σημείο 6) της οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([10])·

14) «ενσωματωμένη πολιτική γνωστοποίησης» σύνολο κανόνων, ενσωματωμένων σε ηλεκτρονική βεβαίωση χαρακτηριστικών από τον πάροχο, το οποίο υποδεικνύει τις προϋποθέσεις που πρέπει να πληροί ένα βασιζόμενο σε πορτοφόλι μέρος για να έχει πρόσβαση στην ηλεκτρονική βεβαίωση χαρακτηριστικών.

## ΚΕΦΑΛΑΙΟ ΙΙ

## ΕΘΝΙΚΑ ΣΧΗΜΑΤΑ ΠΙΣΤΟΠΟΙΗΣΗΣ

### *Άρθρο 3*

### Θέσπιση εθνικών σχημάτων πιστοποίησης

1. Τα κράτη μέλη ορίζουν έναν ιδιοκτήτη σχήματος για κάθε εθνικό σχήμα πιστοποίησης.

2. Το αντικείμενο της πιστοποίησης που ορίζεται στα εθνικά σχήματα πιστοποίησης είναι η παροχή και η λειτουργία υλοποιήσεων πορτοφολιού και των σχημάτων ηλεκτρονικής ταυτοποίησης στο πλαίσιο των οποίων αυτές παρέχονται.

3. Σύμφωνα με τον εκτελεστικό κανονισμό (ΕΕ) 2015/1502, το αντικείμενο της πιστοποίησης στα εθνικά σχήματα πιστοποίησης περιλαμβάνει τα ακόλουθα στοιχεία:

α) τα συστατικά στοιχεία λογισμικού, συμπεριλαμβανομένων των ρυθμίσεων και των διαμορφώσεων υλοποίησης πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχονται οι υλοποιήσεις πορτοφολιού·

β) τα συστατικά στοιχεία υλισμικού και τις πλατφόρμες στις οποίες λειτουργούν τα συστατικά στοιχεία λογισμικού που αναφέρονται στο σημείο β) ή στις οποίες βασίζονται για κρίσιμες λειτουργίες, σε περιπτώσεις στις οποίες παρέχονται άμεσα ή έμμεσα από την υλοποίηση πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχεται η εν λόγω υλοποίηση, και όταν απαιτείται να πληρούν το επιθυμητό επίπεδο διασφάλισης για τα εν λόγω συστατικά στοιχεία λογισμικού. Όταν τα συστατικά στοιχεία υλισμικού και οι πλατφόρμες δεν παρέχονται από τον πάροχο πορτοφολιού, τα εθνικά σχήματα πιστοποίησης διατυπώνουν παραδοχές για την αξιολόγηση των συστατικών στοιχείων υλισμικού και των πλατφορμών, βάσει των οποίων μπορεί να παρέχεται αντίσταση έναντι επιθέσεων υψηλού κινδύνου σύμφωνα με τον εκτελεστικό κανονισμό (ΕΕ) 2015/1502, και προσδιορίζουν τις δραστηριότητες αξιολόγησης για την επιβεβαίωση των εν λόγω παραδοχών, όπως αναφέρεται στο παράρτημα IV·

([10]) Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (ΕΕ L 333 της 27.12.2022, σ. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

γ) τις διαδικασίες που υποστηρίζουν την παροχή και τη λειτουργία μιας υλοποίησης πορτοφολιού, συμπεριλαμβανομένης της διαδικασίας ένταξης χρηστών όπως αναφέρεται στο άρθρο 5α του κανονισμού (ΕΕ) αριθ. 910/2014, καλύπτοντας τουλάχιστον την καταχώριση, τη διαχείριση μέσων ηλεκτρονικής ταυτοποίησης και την οργάνωση σύμφωνα με τα σημεία 2.1, 2.2 και 2.4 του παραρτήματος Ι του εκτελεστικού κανονισμού (ΕΕ) 2015/1502.

4. Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν περιγραφή της συγκεκριμένης αρχιτεκτονικής των υλοποιήσεων πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται. Όταν τα εθνικά σχήματα πιστοποίησης καλύπτουν περισσότερες από μία συγκεκριμένες αρχιτεκτονικές, περιλαμβάνουν προφίλ για κάθε συγκεκριμένη αρχιτεκτονική.

5. Για κάθε προφίλ, τα εθνικά σχήματα πιστοποίησης καθορίζουν τουλάχιστον τα ακόλουθα:

α) τη συγκεκριμένη αρχιτεκτονική μιας υλοποίησης πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται·

β) τις διαδικασίες ασφάλειας που συνδέονται με τα επίπεδα διασφάλισης που ορίζονται στο άρθρο 8 του κανονισμού (ΕΕ) αριθ. 910/2014·

γ) σχέδιο αξιολόγησης που καταρτίζεται σύμφωνα με το τμήμα 7.4.1 του προτύπου EN ISO/IEC 17065·2012·

δ) τις απαιτήσεις ασφάλειας που είναι απαραίτητες για την αντιμετώπιση των κινδύνων και των απειλών κυβερνοασφάλειας που περιλαμβάνονται στο μητρώο κινδύνων που αναφέρεται στο παράρτημα Ι του παρόντος κανονισμού, έως το απαιτούμενο επίπεδο διασφάλισης, και για την επίτευξη κατά περίπτωση των στόχων που ορίζονται στο άρθρο 51 του κανονισμού (ΕΕ) 2019/881·

ε) χαρτογράφηση των ελέγχων που αναφέρονται στο σημείο β) της παρούσας παραγράφου στις συνιστώσες της αρχιτεκτονικής·

στ) περιγραφή του τρόπου με τον οποίο οι διαδικασίες ασφάλειας, η χαρτογράφηση, οι απαιτήσεις ασφάλειας και το σχέδιο αξιολόγησης που αναφέρονται στα στοιχεία β) και γ) επιτρέπουν στους παρόχους υλοποιήσεων πορτοφολιού και στο σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχονται οι υλοποιήσεις να αντιμετωπίζουν επαρκώς τους κινδύνους και τις απειλές κυβερνοασφάλειας που προσδιορίζονται στο μητρώο κινδύνων που αναφέρεται στο στοιχείο δ), έως το απαιτούμενο επίπεδο διασφάλισης βάσει εκτίμησης κινδύνου για τη βελτίωση και τη συμπλήρωση των κινδύνων και των απειλών που περιλαμβάνονται στο μητρώο με κινδύνους και απειλές που αφορούν ειδικά την αρχιτεκτονική.

6. Στο σχέδιο αξιολόγησης που αναφέρεται στην παράγραφο 5, στοιχείο γ) παρατίθενται δραστηριότητες αξιολόγησης που πρέπει α περιλαμβάνονται στην αξιολόγηση μιας υλοποίησης πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται.

7. Η δραστηριότητα αξιολόγησης που αναφέρεται στην παράγραφο 6 απαιτεί από τους παρόχους υλοποιήσεων πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτές παρέχονται να παρέχουν πληροφορίες οι οποίες πληρούν τις απαιτήσεις που παρατίθενται στο παράρτημα ΙΙ.

*Άρθρο 4*

**Γενικές απαιτήσεις**

1. Τα εθνικά σχήματα πιστοποίησης καλύπτουν τις λειτουργικές απαιτήσεις, τις απαιτήσεις κυβερνοασφάλειας και τις απαιτήσεις προστασίας των δεδομένων χρησιμοποιώντας, εφόσον είναι διαθέσιμα και κατά περίπτωση, τα ακόλουθα σχήματα πιστοποίησης:

α) ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας που έχουν δημιουργηθεί δυνάμει του κανονισμού (ΕΕ) 2019/881, συμπεριλαμβανομένου του EUCC·

β) εθνικά σχήματα πιστοποίησης της κυβερνοασφάλειας που καλύπτονται από το EUCC, σύμφωνα με το άρθρο 49 του εκτελεστικού κανονισμού (ΕΕ) 2024/482.

2. Τα εθνικά σχήματα πιστοποίησης μπορούν, επιπλέον, εφόσον είναι διαθέσιμα και κατά περίπτωση, να παραπέμπουν σε:

α) άλλα σχετικά εθνικά σχήματα πιστοποίησης·

β) διεθνή, ευρωπαϊκά και εθνικά πρότυπα·

γ) τεχνικές προδιαγραφές που πληρούν τις απαιτήσεις που ορίζονται στο παράρτημα ΙΙ του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([11]).

3. Τα εθνικά σχήματα πιστοποίησης:

α) προσδιορίζουν τα στοιχεία που παρατίθενται στο τμήμα 6.5 του προτύπου EN ISO/IEC 17067:2013·

β) εφαρμόζονται ως σχήμα τύπου 6, σύμφωνα με το τμήμα 5.3.8 του προτύπου EN ISO/IEC 17067:2013.

4. Τα εθνικά σχήματα πιστοποίησης πληρούν τις ακόλουθες απαιτήσεις:

α) μόνο οι πάροχοι που αναφέρονται στο άρθρο 5α παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 είναι επιλέξιμοι για την έκδοση πιστοποιητικών στο πλαίσιο των εθνικών σχημάτων πιστοποίησης·

β) μόνο το σήμα εμπιστοσύνης χρησιμοποιείται ως σήμα συμμόρφωσης·

γ) οι πάροχοι υλοποιήσεων πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχονται οι υλοποιήσεις περιλαμβάνουν παραπομπές στον κανονισμό (ΕΕ) αριθ. 910/2014 και στον παρόντα κανονισμό όταν αναφέρονται στο σύστημα·

δ) οι πάροχοι υλοποιήσεων πορτοφολιών και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτές παρέχονται συμπληρώνουν την εκτίμηση κινδύνου του σχήματος, όπως αναφέρεται στο άρθρο 3, παράγραφος 5 στοιχείο στ), προκειμένου να εντοπίζουν κινδύνους και απειλές που αφορούν ειδικά την εφαρμογή τους και να προτείνουν κατάλληλα μέτρα αντιμετώπισης για όλους τους σχετικούς κινδύνους και απειλές·

ε) καθορίζονται οι αρμοδιότητες και οι νομικές ενέργειες και περιλαμβάνονται αναφορές στην ισχύουσα εθνική νομοθεσία, η οποία καθορίζει τις αρμοδιότητες και τις πιθανές νομικές ενέργειες, όταν η πιστοποίηση στο πλαίσιο του σχήματος χρησιμοποιείται δολίως.

5. Η αξιολόγηση που αναφέρεται στην παράγραφο 4 στοιχείο δ) κοινοποιείται στον οργανισμό πιστοποίησης για αξιολόγηση.

*Άρθρο 5*

**Διαχείριση περιστατικών και τρωτών σημείων**

1. Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν απαιτήσεις διαχείρισης περιστατικών και τρωτών σημείων σύμφωνα με τις παραγράφους 2 έως 9.

2. Ο κάτοχος πιστοποιητικού συμμόρφωσης μιας υλοποίησης πορτοφολιού και ενός συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται ενημερώνει αμελλητί τον οργανισμό πιστοποίησής τους για οποιαδήποτε παραβίαση ή έκθεση σε κίνδυνο της υλοποίησης πορτοφολιού, ή του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται, η οποία είναι πιθανό να επηρεάσει τη συμμόρφωσή της με τις απαιτήσεις των εθνικών σχημάτων πιστοποίησης.

3. Ο κάτοχος πιστοποιητικού συμμόρφωσης καταρτίζει, τηρεί και εφαρμόζει πολιτική και διαδικασίες διαχείρισης τρωτών σημείων, λαμβάνοντας υπόψη τις διαδικασίες που ορίζονται σε υφιστάμενα ευρωπαϊκά και διεθνή πρότυπα, συμπεριλαμβανομένου του προτύπου EN ISO/IEC 30111:2019.

4. Ο κάτοχος του πιστοποιητικού συμμόρφωσης κοινοποιεί στον εκδίδοντα οργανισμό πιστοποίησης τα τρωτά σημεία και τις αλλαγές που επηρεάζουν την υλοποίηση πορτοφολιού, βάσει καθορισμένων κριτηρίων σχετικά με τις επιπτώσεις των εν λόγω τρωτών σημείων και αλλαγών.

5. Ο κάτοχος του πιστοποιητικού συμμόρφωσης συντάσσει έκθεση ανάλυσης επιπτώσεων τρωτότητας για κάθε τρωτό σημείο που επηρεάζει τα συστατικά στοιχεία λογισμικού της υλοποίησης πορτοφολιού. Η έκθεση περιλαμβάνει τις ακόλουθες πληροφορίες:

α) τις επιπτώσεις των τρωτών σημείων στην πιστοποιημένη υλοποίηση πορτοφολιού·

β) ενδεχόμενους κινδύνους που συνδέονται με την εγγύτητα ή το ενδεχόμενο επίθεσης·

([11]) Κανονισμός (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2012, σχετικά με την ευρωπαϊκή τυποποίηση, την τροποποίηση των οδηγιών του Συμβουλίου 89/686/ΕΟΚ και 93/15/ΕΟΚ και των οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 94/9/ΕΚ, 94/25/ΕΚ, 95/16/ΕΚ, 97/23/ΕΚ, 98/34/ΕΚ, 2004/22/ΕΚ, 2007/23/ΕΚ, 2009/23/ΕΚ και 2009/105/ΕΚ και την κατάργηση της απόφασης 87/95/ΕΟΚ του Συμβουλίου και της απόφασης αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ) (ΕΕ L 316 της 14.11.2012, σ. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

γ) αν το τρωτό σημείο μπορεί να διορθωθεί με τη χρήση διαθέσιμων μέσων·

δ) όταν το τρωτό σημείο μπορεί να διορθωθεί με τη χρήση διαθέσιμων μέσων, πιθανούς τρόπους διόρθωσης του τρωτού σημείου.

6. Όταν απαιτείται κοινοποίηση βάσει της παραγράφου 4, ο κάτοχος του πιστοποιητικού συμμόρφωσης διαβιβάζει, χωρίς αδικαιολόγητη καθυστέρηση, την έκθεση ανάλυσης επιπτώσεων τρωτότητας που αναφέρεται στην παράγραφο 5 στον οργανισμό πιστοποίησης.

7. Ο κάτοχος πιστοποιητικού συμμόρφωσης καταρτίζει, τηρεί και εφαρμόζει πολιτική διαχείρισης τρωτών σημείων η οποία πληροί τις απαιτήσεις που ορίζονται στο παράρτημα I της πράξης για την κυβερνοανθεκτικότητα ([12]).

8. Τα εθνικά σχήματα πιστοποίησης θεσπίζουν απαιτήσεις γνωστοποίησης τρωτών σημείων που ισχύουν για τους οργανισμούς πιστοποίησης.

9. Ο κάτοχος πιστοποιητικού συμμόρφωσης πρέπει να γνωστοποιεί και να καταχωρίζει κάθε δημοσίως γνωστό και διορθωμένο τρωτό σημείο στη υλοποίηση πορτοφολιού ή σε ένα από τα επιγραμμικά αποθετήρια που αναφέρονται στο παράρτημα V.

*Άρθρο 6*

**Συντήρηση των εθνικών σχημάτων πιστοποίησης**

1. Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν διαδικασία εξέτασης της λειτουργίας τους σε περιοδική βάση. Η εν λόγω διαδικασία αποσκοπεί στην επιβεβαίωση της επάρκειάς τους και στον προσδιορισμό των πτυχών που χρήζουν βελτίωσης, λαμβανομένων υπόψη των παρατηρήσεων των ενδιαφερόμενων μερών.

2. Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν διατάξεις σχετικά με τη συντήρησή τους. Η εν λόγω διαδικασία περιλαμβάνει τουλάχιστον τις ακόλουθες απαιτήσεις:

α) κανόνες για τη διακυβέρνηση του ορισμού και των απαιτήσεων των εθνικών σχημάτων πιστοποίησης·

β) καθορισμό χρονοδιαγραμμάτων για την έκδοση πιστοποιητικών μετά την έγκριση επικαιροποιημένων εκδόσεων των εθνικών σχημάτων πιστοποίησης, τόσο για τα νέα πιστοποιητικά συμμόρφωσης όσο και για πιστοποιητικά που έχουν εκδοθεί στο παρελθόν·

γ) περιοδική εξέταση των εθνικών σχημάτων πιστοποίησης, ώστε να διασφαλίζεται ότι οι απαιτήσεις των εθνικών σχημάτων πιστοποίησης εφαρμόζονται με συνεκτικό τρόπο, λαμβανομένων υπόψη τουλάχιστον των ακόλουθων πτυχών:

— αιτήματα για διευκρινίσεις που απευθύνονται στον ιδιοκτήτη του σχήματος σχετικά με τις απαιτήσεις των εθνικών σχημάτων πιστοποίησης·

— παρατηρήσεις από τους ενδιαφερόμενους φορείς και άλλα ενδιαφερόμενα μέρη·

— ανταπόκριση του ιδιοκτήτη εθνικού σχήματος πιστοποίησης σε αιτήματα παροχής πληροφοριών.

δ) κανόνες για την παρακολούθηση των εγγράφων αναφοράς και των διαδικασιών για την εξέλιξη των εκδόσεων αναφοράς των εθνικών σχημάτων πιστοποίησης, συμπεριλαμβανομένων τουλάχιστον μεταβατικών περιόδων·

ε) διαδικασία για τη διασφάλιση της κάλυψης των πλέον πρόσφατων κινδύνων και απειλών κυβερνοασφάλειας, όπως απαριθμούνται στο μητρώο κινδύνων που παρατίθεται στο παράρτημα I του παρόντος κανονισμού·

στ) διαδικασία για τη διαχείριση άλλων αλλαγών στα εθνικά σχήματα πιστοποίησης.

([12]) Κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) αριθ. 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (πράξη για την κυβερνοανθεκτικότητα) (ΕΕ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Τα εθνικά σχήματα πιστοποίησης περιέχουν απαιτήσεις για τη διενέργεια αξιολογήσεων σε πιστοποιημένα επί του παρόντος προϊόντα εντός ορισμένου χρονικού διαστήματος μετά την αναθεώρηση του σχήματος ή μετά την έκδοση νέων προδιαγραφών ή προτύπων, ή νέων εκδόσεων αυτών, με τις οποίες συμμορφώνονται οι υλοποιήσεις πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται.

ΚΕΦΑΛΑΙΟ III

**ΑΠΑΙΤΗΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΥΣ ΙΔΙΟΚΤΗΤΕΣ ΣΧΗΜΑΤΩΝ**

*Άρθρο 7*

**Γενικές απαιτήσεις**

1. Οι ιδιοκτήτες σχημάτων αναπτύσσουν και συντηρούν εθνικά σχήματα πιστοποίησης και διαχειρίζονται τις δραστηριότητές τους.

2. Οι ιδιοκτήτες σχημάτων μπορούν να αναθέτουν υπεργολαβικά το σύνολο ή μέρος των καθηκόντων τους σε τρίτο. Κατά την ανάθεση σε ιδιώτη, οι ιδιοκτήτες σχημάτων καθορίζουν τα καθήκοντα και τις ευθύνες όλων των μερών της σύμβασης. Οι ιδιοκτήτες σχημάτων παραμένουν υπεύθυνοι για όλες τις δραστηριότητες υπεργολαβίας που εκτελούνται από τους υπεργολάβους τους.

3. Οι ιδιοκτήτες σχημάτων εκτελούν τις οικείες δραστηριότητες παρακολούθησης, κατά περίπτωση, τουλάχιστον βάσει των ακόλουθων πληροφοριών:

α) των πληροφοριών που προέρχονται από οργανισμούς πιστοποίησης, εθνικούς οργανισμούς διαπίστευσης και αρμόδιες αρχές εποπτείας της αγοράς·

β) των πληροφοριών που προκύπτουν από τους ελέγχους και τις έρευνες που διεξάγει η ίδια ή άλλη αρχή·

γ) των καταγγελιών και των προσφυγών που λαμβάνονται δυνάμει του άρθρου 15.

4. Οι ιδιοκτήτες σχημάτων ενημερώνουν την ομάδα συνεργασίας σχετικά με τις αναθεωρήσεις των εθνικών σχημάτων πιστοποίησης. Η εν λόγω κοινοποίηση παρέχει επαρκείς πληροφορίες στην ομάδα συνεργασίας για την έκδοση συστάσεων προς τους ιδιοκτήτες σχημάτων και γνωμοδοτήσεων σχετικά με τα επικαιροποιημένα εθνικά σχήματα πιστοποίησης.

ΚΕΦΑΛΑΙΟ IV

**ΑΠΑΙΤΗΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΥΣ ΠΑΡΟΧΟΥΣ ΛΥΣΕΩΝ ΠΟΡΤΟΦΟΛΙΟΥ ΚΑΙ ΤΟ ΣΥΣΤΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΟΠΟΙΟΥ ΑΥΤΕΣ ΠΑΡΕΧΟΝΤΑΙ**

*Άρθρο 8*

**Γενικές απαιτήσεις**

1. Τα εθνικά σχήματα πιστοποίησης περιέχουν απαιτήσεις κυβερνοασφάλειας βάσει εκτίμησης κινδύνου κάθε συγκεκριμένης υποστηριζόμενης αρχιτεκτονικής. Οι εν λόγω απαιτήσεις κυβερνοασφάλειας αποσκοπούν στην αντιμετώπιση των εντοπισθέντων κινδύνων και απειλών κυβερνοασφάλειας, όπως προσδιορίζονται στο μητρώο κινδύνων που παρατίθεται στο παράρτημα Ι.

2. Σύμφωνα με το άρθρο 5α παράγραφος 23 του κανονισμού (ΕΕ) αριθ. 910/2014, τα εθνικά σχήματα πιστοποίησης απαιτούν οι υλοποιήσεις πορτοφολιών και τα σχήματα ηλεκτρονικής ταυτοποίησης βάσει των οποίων αυτές παρέχονται να είναι ανθεκτικά σε επιθέσεις υψηλού κινδύνου για υψηλό επίπεδο διασφάλισης, όπως αναφέρεται στον εκτελεστικό κανονισμό (ΕΕ) 2015/1502.

3. Τα εθνικά σχήματα πιστοποίησης θεσπίζουν κριτήρια ασφαλείας, τα οποία περιλαμβάνουν τις ακόλουθες απαιτήσεις:

α) Πράξη για την κυβερνοανθεκτικότητα κατά περίπτωση, ή απαιτήσεις, που πληρούν τους στόχους ασφάλειας που ορίζονται στο άρθρο 51 του κανονισμού (ΕΕ) 2019/881·

β) καθορισμός και εφαρμογή πολιτικών και διαδικασιών σχετικά με τη διαχείριση των κινδύνων που συνδέονται με τη λειτουργία υλοποίησης πορτοφολιού, συμπεριλαμβανομένου του εντοπισμού και της εκτίμησης των κινδύνων και του μετριασμού των εντοπισθέντων κινδύνων·

γ) καθορισμός και εφαρμογή πολιτικών και διαδικασιών που σχετίζονται με τη διαχείριση αλλαγών και τη διαχείριση των τρωτών σημείων σύμφωνα με το άρθρο 5 του παρόντος κανονισμού·

δ) θέσπιση και εφαρμογή πολιτικών και διαδικασιών διαχείρισης ανθρώπινων πόρων, συμπεριλαμβανομένων απαιτήσεων σχετικά με την εμπειρογνωσία, την αξιοπιστία, την πείρα, την κατάρτιση στον τομέα της ασφάλειας και τα προσόντα του προσωπικού που συμμετέχει στην ανάπτυξη ή τη λειτουργία της υλοποίησης πορτοφολιού·

ε) απαιτήσεις σχετικά με το περιβάλλον λειτουργίας της υλοποίησης πορτοφολιού, μεταξύ άλλων με τη μορφή παραδοχών σχετικά με την ασφάλεια των διατάξεων και των πλατφορμών στις οποίες λειτουργούν τα συστατικά στοιχεία λογισμικού της υλοποίησης πορτοφολιού, συμπεριλαμβανομένων των WSCD και, κατά περίπτωση, των απαιτήσεων αξιολόγησης της συμμόρφωσης για να επιβεβαιωθεί ότι οι εν λόγω παραδοχές επαληθεύονται στις σχετικές διατάξεις και πλατφόρμες·

στ) για κάθε παραδοχή που δεν υποστηρίζεται από πιστοποιητικό συμμόρφωσης ή άλλες αποδεκτές πληροφορίες διασφάλισης, περιγραφή του μηχανισμού τον οποίο χρησιμοποιεί ο πάροχος πορτοφολιού για την επιβολή της παραδοχής, καθώς και αιτιολόγηση ότι ο μηχανισμός είναι επαρκής για να διασφαλίσει την επαλήθευση της παραδοχής·

ζ) θέσπιση και εφαρμογή μέτρων για τη διασφάλιση της χρήσης μιας πιστοποιημένης επί του παρόντος έκδοσης της υλοποίησης πορτοφολιού.

4. Τα εθνικά σχήματα πιστοποίησης περιέχουν λειτουργικές απαιτήσεις σχετικά με τους μηχανισμούς επικαιροποίησης για κάθε συστατικό στοιχείο λογισμικού υλοποιήσεων πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται για τις λειτουργίες που παρατίθενται στο παράρτημα III.

5. Τα εθνικά σχήματα πιστοποίησης απαιτούν οι ακόλουθες πληροφορίες και έγγραφα να παρέχονται ή να τίθενται με άλλο τρόπο στη διάθεση του οργανισμού πιστοποίησης από τον αιτούντα πιστοποίηση:

α) αποδεικτικά στοιχεία σχετικά με τις πληροφορίες που αναφέρονται στο παράρτημα IV σημείο 1, συμπεριλαμβανομένων, κατά περίπτωση, λεπτομερειών σχετικά με την υλοποίηση πορτοφολιού και τον πηγαίο κώδικά της, συμπεριλαμβανομένων των εξής:

— *πληροφορίες αρχιτεκτονικής:* για κάθε συστατικό στοιχείο της υλοποίησης πορτοφολιού (συμπεριλαμβανομένων των συστατικών στοιχείων προϊόντων, διεργασιών και υπηρεσιών), περιγραφή των βασικών ιδιοτήτων ασφαλείας του, συμπεριλαμβανομένων των εξωτερικών εξαρτήσεών του·

— *έλεγχοι και επίπεδα διασφάλισης:* για κάθε έλεγχο ασφάλειας της υλοποίησης πορτοφολιού, περιγραφή του ελέγχου και του απαιτούμενου επιπέδου διασφάλισης, με βάση το παράρτημα του εκτελεστικού κανονισμού (ΕΕ) 2015/1502, το οποίο καθορίζει ορισμένες τεχνικές προδιαγραφές και διαδικασίες που ισχύουν για τους διάφορους ελέγχους που εφαρμόζονται από τα μέσα ηλεκτρονικής ταυτοποίησης·

— *χαρτογράφηση των ελέγχων σε συστατικά στοιχεία αρχιτεκτονικής:* περιγραφή του τρόπου με τον οποίο εφαρμόζονται οι έλεγχοι του πορτοφολιού με χρήση των διαφόρων συστατικών στοιχείων της υλοποίησης πορτοφολιού, βάσει σκεπτικού που εξηγεί τον λόγο για τον οποίο απαιτείται ένα συγκεκριμένο επίπεδο διασφάλισης και τον τρόπο με τον οποίο ο έλεγχος εφαρμόζεται με όλες τις απαιτούμενες πτυχές ασφάλειας στο κατάλληλο επίπεδο·

— *σκεπτικό και αιτιολόγηση της κάλυψης κινδύνων:* αιτιολόγηση για:

— τη χαρτογράφηση των ελέγχων σε κατασκευαστικά στοιχεία·

— την καταλληλότητα του προτεινόμενου σχεδίου αξιολόγησης για την κατάλληλη κάλυψη όλων των ελέγχων·

— την κάλυψη που παρέχουν οι έλεγχοι των κινδύνων και των απειλών κυβερνοασφάλειας που εντοπίζονται στο μητρώο κινδύνων, σε συνδυασμό με ελέγχους των κινδύνων και των απειλών που αφορούν ειδικά την εφαρμογή, στο κατάλληλο επίπεδο διασφάλισης·

β) πληροφορίες που αναφέρονται στο παράρτημα V·

γ) πλήρης κατάλογος των πιστοποιητικών συμμόρφωσης και άλλων πληροφοριών διασφάλισης που χρησιμοποιούνται ως αποδεικτικά στοιχεία κατά τις δραστηριότητες αξιολόγησης·

δ) κάθε άλλη πληροφορία σχετική με τις δραστηριότητες αξιολόγησης.

ΚΕΦΑΛΑΙΟ V

**ΑΠΑΙΤΗΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΥΣ ΟΡΓΑΝΙΣΜΟΥΣ ΠΙΣΤΟΠΟΙΗΣΗΣ**

*Άρθρο 9*

**Γενικές απαιτήσεις**

1. Οι οργανισμοί πιστοποίησης διαπιστεύονται από τους εθνικούς οργανισμούς διαπίστευσης που ορίζονται δυνάμει του κανονισμού (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [13] σύμφωνα με το πρότυπο EN ISO/IEC 17065:2012, υπό την προϋπόθεση ότι πληρούν τις απαιτήσεις που ορίζονται στα εθνικά σχήματα πιστοποίησης σύμφωνα με την παράγραφο 2.

2. Για τους σκοπούς της διαπίστευσης, οι οργανισμοί πιστοποίησης πληρούν όλες τις ακόλουθες απαιτήσεις επάρκειας:

α) λεπτομερείς και τεχνικές γνώσεις των σχετικών αρχιτεκτονικών μιας υλοποίησης πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται, καθώς και των απειλών και των κινδύνων που σχετίζονται με τις εν λόγω αρχιτεκτονικές·

β) γνώση των διαθέσιμων υλοποιήσεων ασφάλειας και των ιδιοτήτων τους σύμφωνα με το παράρτημα του εκτελεστικού κανονισμού (ΕΕ) 2015/1502·

γ) γνώση των δραστηριοτήτων που εκτελούνται δυνάμει πιστοποιητικών συμμόρφωσης που εφαρμόζονται στα συστατικά στοιχεία της υλοποίησης πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης βάσει του οποίου αυτή παρέχεται, ως αντικείμενο πιστοποίησης·

δ) λεπτομερής γνώση του εφαρμοστέου εθνικού σχήματος πιστοποίησης, όπως καθορίζεται σύμφωνα με το κεφάλαιο ΙΙ.

3. Οι οργανισμοί πιστοποίησης εκτελούν τις δραστηριότητες εποπτείας τους ιδίως βάσει των ακόλουθων πληροφοριών:

α) των πληροφοριών που προέρχονται από εθνικούς οργανισμούς διαπίστευσης και αρμόδιες αρχές εποπτείας της αγοράς·

β) των πληροφοριών που προκύπτουν από τους ελέγχους και τις έρευνες που διεξάγει η ίδια ή άλλη αρχή·

γ) των καταγγελιών και των προσφυγών που λαμβάνονται δυνάμει του άρθρου 15.

*Άρθρο 10*

**Υπεργολαβία**

Οι οργανισμοί πιστοποίησης μπορούν να αναθέτουν υπεργολαβικά τις δραστηριότητες αξιολόγησης, όπως ορίζονται στο άρθρο 13, σε τρίτους. Όταν οι δραστηριότητες αξιολόγησης ανατίθενται υπεργολαβικά, τα εθνικά σχήματα πιστοποίησης εξακριβώνουν τα ακόλουθα:

1) όλοι οι υπεργολάβοι του οργανισμού πιστοποίησης που εκτελούν δραστηριότητες αξιολόγησης πληρούν, κατά περίπτωση και όπως ενδείκνυται για τις δραστηριότητες που πρόκειται να εκτελεστούν, τις απαιτήσεις εναρμονισμένων προτύπων όπως το EN ISO/IEC 17025:2017 για τις δοκιμές, το EN ISO/IEC 17020:2012 για την επιθεώρηση, το EN ISO/IEC 17021-1:2015 για τον λογιστικό έλεγχο και το EN ISO/IEC 17029: 2019 για επικύρωση και επαλήθευση·

2) οι οργανισμοί πιστοποίησης αναλαμβάνουν την ευθύνη για όλες τις δραστηριότητες αξιολόγησης που ανατίθενται σε άλλους φορείς και αποδεικνύουν ότι έχουν λάβει κατάλληλα μέτρα κατά τη διάρκεια της διαπίστευσής τους, μεταξύ άλλων βασιζόμενοι στη διαπίστευση των υπεργολάβων τους, κατά περίπτωση·

3) ο βαθμός στον οποίο η προηγούμενη συμφωνία για τις ανάγκες εξωτερικής ανάθεσης λαμβάνεται από τους ιδιοκτήτες του σχήματος ή από τον πελάτη του οποίου η υλοποίηση πορτοφολιού πιστοποιείται στο πλαίσιο του σχήματος πιστοποίησης.

[13] Κανονισμός (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για τον καθορισμό των απαιτήσεων διαπίστευσης και εποπτείας της αγοράς όσον αφορά την εμπορία των προϊόντων και για την κατάργηση του κανονισμού (ΕΟΚ) αριθ. 339/93 (ΕΕ L 218 της 13.8.2008, σ. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

*Άρθρο 11*

**Κοινοποίηση στον εποπτικό φορέα**

Οι οργανισμοί πιστοποίησης κοινοποιούν στον εποπτικό φορέα που αναφέρεται στο άρθρο 46α παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014 την έκδοση, την αναστολή και την ακύρωση των πιστοποιητικών συμμόρφωσης υλοποιήσεων πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται.

*Άρθρο 12*

**Διαχείριση περιστατικών και τρωτών σημείων**

1. Οι οργανισμοί πιστοποίησης αναστέλλουν, χωρίς αδικαιολόγητη καθυστέρηση, το πιστοποιητικό συμμόρφωσης των υλοποιήσεων πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης βάσει του οποίου αυτές παρέχονται, εφόσον βεβαιωθούν ότι η κοινοποιηθείσα παραβίαση ή υπονόμευση της ασφάλειας επηρεάζει τη συμμόρφωσή του με τις απαιτήσεις των εθνικών σχημάτων πιστοποίησης, της υλοποίησης πορτοφολιού ή του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται.

2. Οι οργανισμοί πιστοποίησης ακυρώνουν το πιστοποιητικό συμμόρφωσης που έχει ανασταλεί λόγω παραβίασης ή υπονόμευσης της ασφάλειας που δεν έχει αποκατασταθεί εγκαίρως.

3. Οι οργανισμοί πιστοποίησης ακυρώνουν τα πιστοποιητικά συμμόρφωσης όταν μια εντοπισθείσα τρωτότητα δεν έχει αποκατασταθεί εγκαίρως ανάλογα με τη σοβαρότητα και τις πιθανές επιπτώσεις της, σύμφωνα με το άρθρο 5γ παράγραφος 4 και το άρθρο 5ε παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014.

ΚΕΦΑΛΑΙΟ VI

**ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΕΚΤΙΜΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ**

*Άρθρο 13*

**Δραστηριότητες αξιολόγησης**

1. Τα εθνικά σχήματα πιστοποίησης περιέχουν μεθόδους και διαδικασίες που πρέπει να χρησιμοποιούνται από τους οργανισμούς αξιολόγησης της συμμόρφωσης κατά τη διεξαγωγή των δραστηριοτήτων αξιολόγησής τους σύμφωνα με το πρότυπο EN ISO/IEC 17065:2012, το οποίο καλύπτει τουλάχιστον τις ακόλουθες πτυχές:

α) τις μεθόδους και τις διαδικασίες για τη διεξαγωγή δραστηριοτήτων αξιολόγησης, συμπεριλαμβανομένων εκείνων που σχετίζονται με τη WSCD, όπως ορίζονται στο παράρτημα IV·

β) τον έλεγχο της εφαρμογής της υλοποίησης πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται, με βάση το μητρώο κινδύνων, όπως ορίζεται στο παράρτημα I και συμπληρώνεται, όπου απαιτείται, από ειδικούς κινδύνους εφαρμογής·

γ) δραστηριότητες λειτουργικών δοκιμών, με βάση, εφόσον είναι διαθέσιμες και κατάλληλες, σειρές δοκιμών που καθορίζονται σύμφωνα με τεχνικές προδιαγραφές ή πρότυπα·

δ) αξιολόγηση της ύπαρξης και της καταλληλότητας των διαδικασιών συντήρησης, συμπεριλαμβανομένης τουλάχιστον της διαχείρισης εκδόσεων, της διαχείρισης επικαιροποιήσεων και της διαχείρισης τρωτών σημείων·

ε) αξιολόγηση της λειτουργικής αποτελεσματικότητας των διαδικασιών συντήρησης, συμπεριλαμβανομένης τουλάχιστον της διαχείρισης εκδόσεων, της διαχείρισης επικαιροποιήσεων και της διαχείρισης τρωτών σημείων·

στ) ανάλυση εξάρτησης που παρέχεται από τον πάροχο πορτοφολιού, συμπεριλαμβανομένης μεθοδολογίας για την αξιολόγηση της αποδοχής των πληροφοριών διασφάλισης, η οποία περιλαμβάνει τα στοιχεία που παρατίθενται στο παράρτημα VI·

ζ) αξιολόγηση τρωτότητας, στο κατάλληλο επίπεδο, συμπεριλαμβανομένων των εξής:

— επανεξέταση του σχεδιασμού της υλοποίησης πορτοφολιού και, κατά περίπτωση, του πηγαίου κώδικά της·

— δοκιμή της αντίστασης της υλοποίησης πορτοφολιού έναντι επιθέσεων υψηλού κινδύνου για «υψηλό» επίπεδο διασφάλισης σύμφωνα με το σημείο 2.2.1 του παραρτήματος του εκτελεστικού κανονισμού (ΕΕ) 2015/1502·

η) αξιολόγηση της εξέλιξης του περιβάλλοντος απειλών και των επιπτώσεών του στην κάλυψη των κινδύνων από την υλοποίηση πορτοφολιού, προκειμένου να προσδιοριστούν οι δραστηριότητες αξιολόγησης που απαιτούνται για τα διάφορα συστατικά στοιχεία της υλοποίησης πορτοφολιού.

2. Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν αξιολόγηση στο πλαίσιο της οποίας εξακριβώνεται αν η εφαρμογή υλοποιήσεων πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτές παρέχονται αντιστοιχεί στην αρχιτεκτονική που ορίζεται στο άρθρο 3 παράγραφος 5 στοιχείο α), καθώς και αξιολόγηση στο πλαίσιο της οποίας προσδιορίζεται αν το προτεινόμενο σχέδιο αξιολόγησης μαζί με την υλοποίηση αντιστοιχεί στο σχέδιο αξιολόγησης που αναφέρεται στο άρθρο 3 παράγραφος 5 στοιχείο γ).

3. Τα εθνικά σχήματα πιστοποίησης καθορίζουν κανόνες δειγματοληψίας, προκειμένου να αποφεύγεται η επανάληψη πανομοιότυπων δραστηριοτήτων αξιολόγησης και να δίνεται έμφαση σε δραστηριότητες που αφορούν ειδικά μια συγκεκριμένη παραλλαγή. Οι εν λόγω κανόνες δειγματοληψίας επιτρέπουν τη διενέργεια λειτουργικών δοκιμών και δοκιμών ασφάλειας μόνο σε δείγμα παραλλαγώνενός συστατικού στοιχείου-στόχου μιας υλοποίησης πορτοφολιού και στο σύστημα ηλεκτρονικής ταυτοποίησης βάσει του οποίου αυτή παρέχεται, καθώς και σε δείγμα διατάξεων-στόχων. Τα εθνικά σχήματα πιστοποίησης απαιτούν από όλους τους οργανισμούς πιστοποίησης να αιτιολογούν τη χρήση δειγματοληψίας.

4. Τα εθνικά σχήματα πιστοποίησης απαιτούν την αξιολόγηση, από τον οργανισμό πιστοποίησης, της WSCA με βάση τις μεθόδους και τις διαδικασίες που ορίζονται στο παράρτημα IV.

*Άρθρο 14*

**Δραστηριότητες πιστοποίησης**

1. Τα εθνικά σχήματα πιστοποίησης προβλέπουν δραστηριότητα πιστοποίησης για τον σκοπό της έκδοσης πιστοποιητικού συμμόρφωσης, σύμφωνα με το τμήμα V στοιχείο α) του προτύπου EN ISO/IEC 17067:2013, πίνακας 1, συμπεριλαμβανομένων των ακόλουθων πτυχών:

α) του περιεχομένου του πιστοποιητικού συμμόρφωσης όπως καθορίζεται στο παράρτημα VII·

β) του τρόπου με τον οποίο πρέπει να αναφέρονται τα αποτελέσματα της αξιολόγησης στη δημόσια έκθεση πιστοποίησης, η οποία πρέπει τουλάχιστον να περιλαμβάνει περίληψη του προκαταρκτικού σχεδίου ελέγχου και επικύρωσης, όπως ορίζεται στο παράρτημα VIII·

γ) του περιεχομένου των αποτελεσμάτων της αξιολόγησης που αναφέρονται στην έκθεση αξιολόγησης της πιστοποίησης, συμπεριλαμβανομένων των στοιχείων που ορίζονται στο παράρτημα VIII.

2. Η έκθεση αξιολόγησης της πιστοποίησης μπορεί να τίθεται στη διάθεση της ομάδας συνεργασίας και της Επιτροπής.

*Άρθρο 15*

**Καταγγελίες και προσφυγές**

Τα εθνικά σχήματα πιστοποίησης περιέχουν διαδικασίες ή παραπομπές στην ισχύουσα εθνική νομοθεσία, οι οποίες καθορίζουν τον μηχανισμό για την αποτελεσματική υποβολή και διεκπεραίωση καταγγελιών και προσφυγών σε σχέση με την εκ μέρους τους εφαρμογή του σχήματος πιστοποίησης ή το εκδοθέν πιστοποιητικό συμμόρφωσης. Οι διαδικασίες αυτές περιλαμβάνουν την ενημέρωση του καταγγέλλοντος σχετικά με την πρόοδο της διαδικασίας και τη ληφθείσα απόφαση, καθώς και την ενημέρωση του καταγγέλλοντος σχετικά με το δικαίωμα πραγματικής προσφυγής. Τα εθνικά σχήματα πιστοποίησης απαιτούν να διαβιβάζονται στον ιδιοκτήτη του σχήματος προς αξιολόγηση και επίλυση όλες οι καταγγελίες και προσφυγές που δεν έχουν επιλυθεί ή δεν μπορούν να επιλυθούν από τον οργανισμό πιστοποίησης.

*Άρθρο 16*

**Δραστηριότητες εποπτείας**

1. Τα εθνικά σχήματα πιστοποίησης απαιτούν από τους οργανισμούς πιστοποίησης να εκτελούν δραστηριότητες εποπτείας που συνίστανται στην εποπτική αξιολόγηση των διαδικασιών σε συνδυασμό με τυχαίες δοκιμές ή επιθεωρήσεις.

2. Τα εθνικά σχήματα πιστοποίησης περιέχουν απαιτήσεις βάσει των οποίων οι ιδιοκτήτες σχημάτων πρέπει να παρακολουθούν τη συμμόρφωση των οργανισμών πιστοποίησης με τις υποχρεώσεις τους σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014 και σύμφωνα με τα εθνικά σχήματα πιστοποίησης, κατά περίπτωση.

3. Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν απαιτήσεις βάσει των οποίων οι οργανισμοί πιστοποίησης πρέπει να παρακολουθούν τα εξής:

α) τη συμμόρφωση των κατόχων πιστοποιητικού συμμόρφωσης που έχει εκδοθεί στο πλαίσιο εθνικών σχημάτων πιστοποίησης με τις υποχρεώσεις τους όσον αφορά την πιστοποίηση σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014 και σύμφωνα με τα εθνικά σχήματα πιστοποίησης·

β) τη συμμόρφωση της πιστοποιημένης υλοποίησης πορτοφολιού με τις απαιτήσεις που ορίζονται στα εθνικά σχήματα πιστοποίησης.

*Άρθρο 17*

**Συνέπειες της μη συμμόρφωσης**

Τα εθνικά σχήματα πιστοποίησης καθορίζουν τις συνέπειες της μη συμμόρφωσης μιας πιστοποιημένης υλοποίησης πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται, με τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Οι συνέπειες αυτές περιλαμβάνουν τις εξής πτυχές:

1) την υποχρέωση του οργανισμού πιστοποίησης να ενημερώνει τον κάτοχο του πιστοποιητικού συμμόρφωσης και να ζητεί από τον κάτοχο του πιστοποιητικού συμμόρφωσης να εφαρμόσει διορθωτικά μέτρα·

2) την υποχρέωση του οργανισμού πιστοποίησης να ενημερώνει άλλες αρμόδιες αρχές εποπτείας της αγοράς όταν η μη συμμόρφωση αφορά σχετική νομοθεσία της Ένωσης·

3) τους όρους για τη λήψη διορθωτικών μέτρων από τον κάτοχο του πιστοποιητικού συμμόρφωσης·

4) τους όρους για την αναστολή του πιστοποιητικού συμμόρφωσης από τον οργανισμό πιστοποίησης και για την αποκατάσταση του πιστοποιητικού συμμόρφωσης μετά τη διόρθωση της μη συμμόρφωσης·

5) τους όρους ακύρωσης του πιστοποιητικού συμμόρφωσης από τον οργανισμό πιστοποίησης·

6) τις συνέπειες της μη συμμόρφωσης του οργανισμού πιστοποίησης με τις απαιτήσεις του εθνικού σχήματος πιστοποίησης.

ΚΕΦΑΛΑΙΟ VII

**ΚΥΚΛΟΣ ΖΩΗΣ ΤΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ**

*Άρθρο 18*

**Κύκλος ζωής της πιστοποίησης**

1. Η ισχύς των πιστοποιητικών συμμόρφωσης που εκδίδονται στο πλαίσιο των εθνικών σχημάτων πιστοποίησης υπόκειται σε δραστηριότητες τακτικής αξιολόγησης από τον οργανισμό πιστοποίησης, οι οποίες εκτελούνται σύμφωνα με τις απαιτήσεις που ορίζονται στο παράρτημα IX.

2. Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν διαδικασία για την επαναπιστοποίηση υλοποιήσεων πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτές παρέχονται, κατόπιν αιτήματος του κατόχου του πιστοποιητικού συμμόρφωσης πριν από τη λήξη του αρχικού πιστοποιητικού συμμόρφωσης. Η εν λόγω διαδικασία επαναπιστοποίησης περιλαμβάνει πλήρη αξιολόγηση της υλοποίησης πορτοφολιού και του συστήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται, συμπεριλαμβανομένης εκτίμησης τρωτότητας, σύμφωνα με τις αρχές που ορίζονται στο παράρτημα IX.

3. Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν διαδικασία για τη διαχείριση των αλλαγών σε μια πιστοποιημένη υλοποίηση πορτοφολιού και στο σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται. Η διαδικασία αυτή περιλαμβάνει κανόνες βάσει των οποίων προσδιορίζεται αν μια αλλαγή πρέπει να καλύπτεται από ειδική αξιολόγηση, όπως αναφέρεται στην παράγραφο 4, ή από την επαλήθευση της λειτουργικής αποτελεσματικότητας των διαδικασιών συντήρησης, όπως αναφέρεται στο παράρτημα IV.

4. Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν διαδικασία για ειδικές αξιολογήσεις σύμφωνα με το πρότυπο EN ISO/IEC 17065:2012. Η εν λόγω διαδικασία για ειδικές αξιολογήσεις περιλαμβάνει επιλογή των δραστηριοτήτων που πρέπει να εκτελούνται για την αντιμετώπιση του συγκεκριμένου ζητήματος που προκάλεσε την ειδική αξιολόγηση.

5. Τα εθνικά σχήματα πιστοποίησης θεσπίζουν κανόνες σχετικά με την ακύρωση ενός πιστοποιητικού συμμόρφωσης.

ΚΕΦΑΛΑΙΟ VIII

**ΤΗΡΗΣΗ ΑΡΧΕΙΩΝ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ**

*Άρθρο 19*

**Τήρηση αρχείων**

1. Τα εθνικά σχήματα πιστοποίησης περιέχουν απαιτήσεις βάσει των οποίων οι οργανισμοί πιστοποίησης πρέπει να δημιουργήσουν σύστημα καταγραφής για όλες τις σχετικές πληροφορίες που παράγονται σε σχέση με τις δραστηριότητες αξιολόγησης της συμμόρφωσης τις οποίες εκτελούν, συμπεριλαμβανομένων των δεδομένων που εκδίδονται και λαμβάνονται από παρόχους υλοποιήσεων πορτοφολιού και των σχημάτων ηλεκτρονικής ταυτοποίησης βάσει των οποίων αυτές παρέχονται. Τα αρχεία των πληροφοριών αυτών αποθηκεύονται με ασφαλή τρόπο. Τα αρχεία μπορούν να τηρούνται ηλεκτρονικά και παραμένουν προσβάσιμα για όσο χρονικό διάστημα απαιτείται από το ενωσιακό ή το εθνικό δίκαιο και για τουλάχιστον πέντε έτη μετά την ακύρωση ή τη λήξη ισχύος του σχετικού πιστοποιητικού συμμόρφωσης.

2. Τα εθνικά σχήματα πιστοποίησης καθορίζουν απαιτήσεις βάσει των οποίων ο κάτοχος του πιστοποιητικού συμμόρφωσης πρέπει να αποθηκεύει με ασφάλεια τις ακόλουθες πληροφορίες για τους σκοπούς του παρόντος κανονισμού και για τουλάχιστον πέντε έτη μετά την ακύρωση ή τη λήξη ισχύος του σχετικού πιστοποιητικού συμμόρφωσης:

α) αρχεία των πληροφοριών που παρασχέθηκαν στον οργανισμό πιστοποίησης ή σε οποιονδήποτε υπεργολάβο του κατά τη διάρκεια της διαδικασίας πιστοποίησης·

β) δείγματα συστατικών στοιχείων υλισμικού που έχουν συμπεριληφθεί στο πεδίο εφαρμογής της πιστοποίησης για την υλοποίηση πορτοφολιού.

3. Τα εθνικά σχήματα πιστοποίησης απαιτούν από τον κάτοχο του πιστοποιητικού συμμόρφωσης να θέτει τις πληροφορίες που αναφέρονται στην παράγραφο 1 στη διάθεση του οργανισμού πιστοποίησης ή του εποπτικού φορέα που αναφέρεται στο άρθρο 46α παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 910/2014, κατόπιν αιτήματος.

*Άρθρο 20*

**Προστασία πληροφοριών**

Στο πλαίσιο των εθνικών σχημάτων πιστοποίησης, όλα τα πρόσωπα ή οι οργανισμοί στους οποίους χορηγείται πρόσβαση σε πληροφορίες κατά την εκτέλεση δραστηριοτήτων στο πλαίσιο του εθνικού σχήματος πιστοποίησης υποχρεούνται να διασφαλίζουν την ασφάλεια και την προστασία του εμπορικού απορρήτου και άλλων εμπιστευτικών πληροφοριών, καθώς και να διαφυλάσσουν τα δικαιώματα διανοητικής ιδιοκτησίας, και να λαμβάνουν τα αναγκαία και κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της εν λόγω εμπιστευτικότητας.

ΚΕΦΑΛΑΙΟ IX

**ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ**

*Άρθρο 21*

**Μετάβαση σε ένα ευρωπαϊκό σχήμα πιστοποίησης της κυβερνοασφάλειας**

Ο παρών κανονισμός υπόκειται σε επανεξέταση, κατά την έγκριση του πρώτου ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας για υλοποιήσεις πορτοφολιού και για τα συστήματα ηλεκτρονικής ταυτοποίησης στο πλαίσιο των οποίων αυτές παρέχονται, με στόχο να ληφθεί υπόψη η συμβολή του εν λόγω ευρωπαϊκού σχήματος πιστοποίησης της κυβερνοασφάλειας στη συνολική πιστοποίηση των υλοποιήσεων πορτοφολιού και των συστημάτων ηλεκτρονικής ταυτοποίησης στο πλαίσιο των οποίων αυτές παρέχονται.

*Άρθρο 22*

**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, 28 Νοεμβρίου 2024.

*Για την Επιτροπή*
*Η Πρόεδρος*
Ursula VON DER LEYEN

*ΠΑΡΑΡΤΗΜΑ Ι*

**ΜΗΤΡΩΟ ΚΙΝΔΥΝΩΝ ΓΙΑ ΤΑ ΕΥΡΩΠΑΪΚΑ ΠΟΡΤΟΦΟΛΙΑ ΨΗΦΙΑΚΗΣ ΤΑΥΤΟΤΗΤΑΣ**

**Εισαγωγή**

Το μητρώο κινδύνων περιγράφει τους κύριους κινδύνους και απειλές για την ασφάλεια και την ιδιωτική ζωή που ισχύουν για τα πορτοφόλια και που αντιμετωπίζονται δεόντως σε κάθε αρχιτεκτονική και εφαρμογή πορτοφολιών. Οι **κίνδυνοι υψηλού επιπέδου** (τμήμα Ι) σχετίζονται με τη χρήση πορτοφολιών από τους χρήστες και τα βασιζόμενα μέρη, και συνδέονται με άμεσες απειλές που στοχεύουν τα περιουσιακά στοιχεία των πορτοφολιών. Επιπλέον, εντοπίζονται ορισμένοι **κίνδυνοι σε επίπεδο συστήματος** (τμήμα ΙΙ) για τα πορτοφόλια, οι οποίοι κατά κανόνα προκύπτουν από συνδυασμό απειλών που ισχύουν για ολόκληρο το σύστημα πορτοφολιών.

| Είδος κινδύνου | Αναγνωριστικός κωδικός κινδύνου | Σχετικοί τίτλοι κινδύνου |
|---|---|---|
| **Κίνδυνοι υψηλού επιπέδου για τα πορτοφόλια** | R1 | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας |
| | R2 | Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας |
| | R3 | Δημιουργία ή χρήση ψευδών χαρακτηριστικών |
| | R4 | Εντοπισμός κλοπής |
| | R5 | Κλοπή δεδομένων |
| | R6 | Γνωστοποίηση δεδομένων |
| | R7 | Παραποίηση δεδομένων |
| | R8 | Απώλεια δεδομένων |
| | R9 | Μη εγκεκριμένη συναλλαγή |
| | R10 | Παραποίηση συναλλαγών |
| | R11 | Αποκήρυξη |
| | R12 | Γνωστοποίηση δεδομένων συναλλαγών |
| | R13 | Διαταραχή στην παροχή υπηρεσίας |
| | R14 | Εποπτεία |
| **Κίνδυνοι που σχετίζονται με το σύστημα** | SR1 | Γενικευμένη εποπτεία |
| | SR2 | Βλάβη της φήμης |
| | SR3 | Μη συμμόρφωση με τη νομοθεσία |

Το μητρώο εντοπίζει επίσης **τεχνικές απειλές** (τμήμα ΙΙΙ) που στοχεύουν στην εφαρμογή της υλοποίησης πορτοφολιού. Οι απειλές αυτές συνδέονται με τους κινδύνους υψηλού επιπέδου, υπό την έννοια ότι σε καθεμία από αυτές ελλοχεύουν, δυνητικά, πολλοί κίνδυνοι υψηλού επιπέδου.

| Είδος απειλής | Αναγνωριστικός κωδικός απειλής | Σχετικοί τίτλοι απειλής | Υποκατηγορίες απειλών |
|---|---|---|---|
| **Τεχνική απειλή** | TT1 | Φυσικές επιθέσεις | 1.1. *Κλοπή* |
| | | | 1.2. *Διαρροή πληροφοριών* |
| | | | 1.3 *Παραποίηση* |
| | TT2 | Σφάλματα και εσφαλμένες διαμορφώσεις | 2.1. *Σφάλματα κατά τη διαχείριση συστήματος ΤΠ* |
| | | | 2.2. *Σφάλματα σε επίπεδο εφαρμογής ή σφάλματα χρήσης* |
| | | | 2.3. *Σφάλματα κατά τον χρόνο ανάπτυξης και εσφαλμένες διαμορφώσεις του συστήματος* |

| Είδος απειλής | Αναγνωριστικός κωδικός απειλής | Σχετικοί τίτλοι απειλής | Υποκατηγορίες απειλών |
|---|---|---|---|
| | TT3 | Χρήση αναξιόπιστων πόρων | 3.1. *Εσφαλμένη χρήση ή διαμόρφωση συστατικών στοιχείων πορτοφολιού* |
| | TT4 | Αστοχία και διακοπές λειτουργίας | 4.1. *Αστοχία ή δυσλειτουργία εξοπλισμού, διατάξεων ή συστημάτων* |
| | | | 4.2. *Απώλεια πόρων* |
| | | | 4.3 *Απώλεια υπηρεσιών υποστήριξης* |
| | TT5 | Κακόβουλες ενέργειες | 5.1 *Υποκλοπή πληροφοριών* |
| | | | 5.2 *Ηλεκτρονικό «ψάρεμα» (phishing) και πλαστοπροσωπία (spoofing)* |
| | | | 5.3 *Αναπαραγωγή μηνυμάτων* |
| | | | 5.4 *Επίθεση ωμής βίας* |
| | | | 5.5 *Τρωτά σημεία λογισμικού* |
| | | | 5.6 *Επιθέσεις στην αλυσίδα εφοδιασμού* |
| | | | 5.7 *Κακόβουλο λογισμικό* |
| | | | 5.8 *Πρόβλεψη τυχαίων αριθμών* |

Τέλος, το μητρώο **περιλαμβάνει τις άμεσες απειλές για τα πορτοφόλια** και καθεμία συνδέεται με (μη εξαντλητική) επιλογή κινδύνων (τμήμα IV).

*ΤΜΗΜΑ I*

***Κίνδυνοι υψηλού επιπέδου για τα πορτοφόλια***

**R1. Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας**

Ως δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας ορίζεται η δημιουργία ηλεκτρονικής ταυτότητας σε πορτοφόλι η οποία υπάρχει στον πραγματικό κόσμο και έχει αποδοθεί σε άλλον χρήστη. Στην ουσία, ο κίνδυνος αυτός οδηγεί σε κινδύνους Κλοπής ταυτότητας (R4) και Μη Εξουσιοδοτημένων συναλλαγών (R9).

**R2. Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας**

Ως δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας ορίζεται η δημιουργία ηλεκτρονικής ταυτότητας σε πορτοφόλι η οποία δεν υπάρχει στον πραγματικό κόσμο.

**R3. Δημιουργία ή χρήση ψευδών χαρακτηριστικών**

Ως δημιουργία ή χρήση ψευδών χαρακτηριστικών ορίζεται η δημιουργία ή η χρήση χαρακτηριστικών που δεν μπορούν να επικυρωθούν για να εκδοθούν από τον υποτιθέμενο πάροχο και δεν μπορούν να θεωρηθούν αξιόπιστα.

**R4. Εντοπισμός κλοπής**

Ως κλοπή ταυτότητας ορίζεται η άνευ αδείας απόκτηση της μονάδας πορτοφολιού ή η απώλεια παραγόντων επαλήθευσης ταυτότητας που επιτρέπουν την οικειοποίηση της ταυτότητας ενός προσώπου.

**R5. Κλοπή δεδομένων**

Ως κλοπή δεδομένων ορίζεται η άνευ αδείας εξαγωγή δεδομένων. Η κλοπή δεδομένων συνδέεται επίσης με απειλές, όπως η υποκλοπή δεδομένων (μη εξουσιοδοτημένη συλλογή δεδομένων υπό διαμετακόμιση) και η αποκρυπτογράφηση δεδομένων (μη εξουσιοδοτημένη αποκωδικοποίηση κρυπτογραφημένων δεδομένων), οι οποίες είναι πιθανό να οδηγήσουν σε ορισμένες περιπτώσεις σε γνωστοποίηση δεδομένων (R6).

**R6. Γνωστοποίηση δεδομένων**

Ως γνωστοποίηση δεδομένων ορίζεται η άνευ αδείας έκθεση δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Ο κίνδυνος παραβίασης της ιδιωτικής ζωής είναι πολύ παρόμοιος όταν εξετάζεται από την άποψη της προστασίας ιδιωτικής ζωής και όχι από την άποψη της ασφάλειας.

**R7. Παραποίηση δεδομένων**

Ως παραποίηση δεδομένων ορίζεται η μη εξουσιοδοτημένη αλλοίωση δεδομένων.

**R8. Απώλεια δεδομένων**

Ως απώλεια δεδομένων ορίζεται η κατάσταση κατά την οποία δεδομένα που είναι αποθηκευμένα στο πορτοφόλι χάνονται λόγω κατάχρησης ή κακόβουλης ενέργειας. Ο κίνδυνος αυτός αποτελεί συχνά δευτερεύοντα κίνδυνο Παραποίησης δεδομένων (R7) ή Διαταραχής στην παροχή υπηρεσίας (R13), όταν δεν είναι δυνατή η αποκατάσταση του συνόλου ή μέρους των δεδομένων.

**R9. Μη εγκεκριμένη συναλλαγή**

Ως μη εγκεκριμένες συναλλαγές ορίζονται οι επιχειρησιακές δραστηριότητες που διεξάγονται χωρίς την άδεια ή τη γνώση του χρήστη πορτοφολιού. Σε πολλές περιπτώσεις, μια μη εγκεκριμένη συναλλαγή μπορεί να οδηγήσει σε Κλοπή ταυτότητας (R4) ή σε γνωστοποίηση δεδομένων (R6). Σχετίζεται επίσης με μη εγκεκριμένες συναλλαγές, όπως η κατάχρηση κρυπτογραφικών κλειδιών.

**R10. Παραποίηση συναλλαγών**

Ως παραποίηση συναλλαγών ορίζεται η μη εξουσιοδοτημένη μεταβολή πράξεων του πορτοφολιού. Η παραποίηση συναλλαγών αποτελεί επίθεση κατά της ακεραιότητας και σχετίζεται με παραβίαση της ακεραιότητας των δεδομένων.

**R11. Αποκήρυξη**

Ως αποκήρυξη ορίζεται η κατάσταση κατά την οποία ένα ενδιαφερόμενο μέρος μπορεί να αρνηθεί να εκτελέσει μια ενέργεια ή να συμμετάσχει σε μια συναλλαγή, και άλλα ενδιαφερόμενα μέρη δεν διαθέτουν κατάλληλα αποδεικτικά στοιχεία για να το αντικρούσουν.

**R12. Γνωστοποίηση δεδομένων συναλλαγών**

Ως γνωστοποίηση δεδομένων συναλλαγών ορίζεται η γνωστοποίηση πληροφοριών που σχετίζονται με πληροφορίες σχετικά με μια συναλλαγή μεταξύ ενδιαφερόμενων μερών.

**R13. Διαταραχή στην παροχή υπηρεσίας**

Ως διαταραχή στην παροχή υπηρεσίας ορίζεται η διακοπή ή υποβάθμιση της κανονικής λειτουργίας του πορτοφολιού. Ένα συγκεκριμένο είδος διαταραχής στην παροχή υπηρεσίας είναι ο αποκλεισμός του χρήστη, ο οποίος ορίζεται ως η αδυναμία ενός χρήστη να έχει πρόσβαση στον λογαριασμό του ή στο πορτοφόλι του.

**R14. Εποπτεία**

Ως εποπτεία ή παρακολούθηση ορίζεται η μη εξουσιοδοτημένη παρακολούθηση ή παρατήρηση των δραστηριοτήτων, των επικοινωνιών ή των δεδομένων ενός χρήστη πορτοφολιού. Η εποπτεία συνδέεται συχνά με συμπερασμό, ο οποίος ορίζεται ως η εξαγωγή ευαίσθητων ή προσωπικών πληροφοριών από φαινομενικά αβλαβή δεδομένα.

*ΤΜΗΜΑ II*

***Κίνδυνοι που σχετίζονται με το σύστημα***

Οι κίνδυνοι αυτοί δεν χρησιμοποιούνται στον κατάλογο των απειλών, καθώς αποτελούν συνήθως συνέπεια πολλαπλών απειλών, οι οποίες επαναλαμβάνονται κατά τρόπο που απειλεί ολόκληρο το σύστημα.

**SR1. Γενικευμένη εποπτεία**

Ως γενικευμένη εποπτεία ορίζεται η παρακολούθηση ή η παρατήρηση των δραστηριοτήτων πολλών χρηστών μέσω της επικοινωνίας ή των δεδομένων του πορτοφολιού τους. Η γενικευμένη εποπτεία συνδέεται συχνά με την εποπτεία (R14) και τον συμπερασμό σε παγκόσμια κλίμακα, όπου πληροφορίες σχετικά με πολλούς χρήστες συνδυάζονται για την εξαγωγή ευαίσθητων δεδομένων ή δεδομένων προσωπικού χαρακτήρα σχετικά με τους χρήστες ή για τον εντοπισμό στατιστικών τάσεων που μπορούν να χρησιμοποιηθούν για τον σχεδιασμό περαιτέρω επιθέσεων.

**SR2. Βλάβη της φήμης**

Ως βλάβη της φήμης ορίζεται η βλάβη που προκαλείται στη φήμη ενός οργανισμού ή κρατικού φορέα. Η βλάβη της φήμης θα απορρέει επίσης από άλλους κινδύνους όταν μια παραβίαση ή ένα περιστατικό καλύπτεται από τα μέσα ενημέρωσης και θέτει τον οργανισμό σε δυσμενή θέση. Η βλάβη της φήμης μπορεί να οδηγήσει σε περαιτέρω κινδύνους, όπως απώλεια εμπιστοσύνης, που απορρέουν από εύλογες αμφιβολίες του χρήστη, και απώλεια οικοσυστήματος, όταν καταρρέει ολόκληρο το οικοσύστημα.

**SR3. Μη συμμόρφωση με τη νομοθεσία**

Ως μη συμμόρφωση με τη νομοθεσία ορίζεται η κατάσταση κατά την οποία δεν μπορούν να τηρηθούν οι σχετικοί νόμοι, κανονισμοί ή πρότυπα. Στο πλαίσιο του πορτοφολιού, δεδομένου ότι η ασφάλεια και η προστασία της ιδιωτικής ζωής στο πλαίσιο της υλοποίησης αποτελούν νομικές απαιτήσεις, όλες οι απειλές είναι πιθανό να οδηγήσουν σε κάποιου είδους μη συμμόρφωση με τη νομοθεσία.

*ΤΜΗΜΑ III*

***Τεχνικές απειλές***

Οι τεχνικές απειλές δεν συνδέονται όλες με συγκεκριμένους κινδύνους στα πορτοφόλια, διότι πολλές από αυτές αποτελούν μέσα που θα μπορούσαν να χρησιμοποιηθούν για την υλοποίηση επιθέσεων που αντιστοιχούν σε πολλούς διαφορετικούς κινδύνους.

**TT1. Φυσικές επιθέσεις**

1.1. *Κλοπή*

Ως κλοπή ορίζεται η κλοπή διατάξεων που ενδέχεται να αλλοιώσει την ορθή λειτουργία του πορτοφολιού (σε περίπτωση που η διάταξη κλαπεί και η μονάδα πορτοφολιού δεν προστατεύεται επαρκώς). Αυτό μπορεί να συμβάλει σε πολλούς κινδύνους, συμπεριλαμβανομένης της Κλοπής ταυτότητας (R4), της Κλοπής δεδομένων (R5) και των Μη Εγκεκριμένων συναλλαγών (R9).

1.2. *Διαρροή πληροφοριών*

Ως διαρροή πληροφοριών ορίζεται η μη εξουσιοδοτημένη πρόσβαση, η έκθεση πληροφοριών ή ο διαμοιρασμός μετά από φυσική πρόσβαση στο πορτοφόλι. Αυτό μπορεί να συμβάλει ιδίως στη γνωστοποίηση δεδομένων (R6) και στην Κλοπή δεδομένων (R5).

1.3. *Παραποίηση*

Ως παραποίηση ορίζεται η παραβίαση της ακεραιότητας ενός ή περισσότερων συστατικών στοιχείων της μονάδας πορτοφολιού ή των συστατικών στοιχείων στα οποία βασίζεται η μονάδα πορτοφολιού, π.χ. η διάταξη χρήστη ή το λειτουργικό της σύστημα. Αυτό μπορεί να συντελέσει ιδίως στην Παραποίηση δεδομένων (R7), στην Απώλεια δεδομένων (R8) και στην Παραποίηση συναλλαγών (R10). Όταν η παραποίηση στοχεύει σε συστατικά στοιχεία λογισμικού, μπορεί να συντελέσει σε πολλούς κινδύνους.

**TT2. Σφάλματα και εσφαλμένες διαμορφώσεις**

2.1. *Σφάλματα κατά τη διαχείριση συστήματος ΤΠ*

Ως σφάλματα κατά τη διαχείριση συστήματος ΤΠ ορίζονται η διαρροή πληροφοριών, ο διαμοιρασμός πληροφοριών ή η ζημία που προκαλείται από την εσφαλμένη χρήση των περιουσιακών στοιχείων ΤΠ από τους χρήστες (έλλειψη ενημέρωσης σχετικά με τα χαρακτηριστικά εφαρμογής) ή από ακατάλληλη διαμόρφωση ή διαχείριση των περιουσιακών στοιχείων ΤΠ.

2.2. *Σφάλματα σε επίπεδο εφαρμογής ή σφάλματα χρήσης*

Ως σφάλματα σε επίπεδο εφαρμογής ή σφάλματα χρήσης ορίζονται οι δυσλειτουργίες της εφαρμογής λόγω σφάλματος στην ίδια την εφαρμογή ή σφάλματος που διαπράττεται από έναν από τους χρήστες (χρήστες πορτοφολιού και βασιζόμενα μέρη).

2.3. *Σφάλματα κατά τον χρόνο ανάπτυξης και εσφαλμένες διαμορφώσεις του συστήματος*

Ως σφάλματα κατά τον χρόνο ανάπτυξης και εσφαλμένες διαμορφώσεις του συστήματος ορίζονται οι δυσλειτουργίες ή τα τρωτά σημεία που προκαλούνται από ακατάλληλα αναπτυγμένους ή διαμορφωμένα περιουσιακά στοιχεία ΤΠ ή επιχειρησιακές διαδικασίες (ακατάλληλες προδιαγραφές προϊόντων ΤΠ, ανεπαρκής χρηστικότητα, μη ασφαλείς διεπαφές, ακατάλληλες ροές πολιτικών και διαδικασιών, σφάλματα σχεδιασμού).

**TT3. Χρήση αναξιόπιστων πόρων**

Ως χρήση αναξιόπιστων πόρων ορίζεται η δραστηριότητα που οδηγεί σε ακούσια ζημία λόγω ασαφών σχέσεων εμπιστοσύνης, όπως η επίδειξη εμπιστοσύνης σε έναν τρίτο πάροχο χωρίς επαρκή διασφάλιση.

3.1. *Εσφαλμένη χρήση ή διαμόρφωση συστατικών στοιχείων πορτοφολιού*

Ως εσφαλμένη χρήση ή διαμόρφωση συστατικών στοιχείων πορτοφολιού ορίζεται η ακούσια ζημία σε συστατικά στοιχεία πορτοφολιού λόγω εσφαλμένης χρήσης ή διαμόρφωσης από χρήστες πορτοφολιού ή από ανεπαρκώς καταρτισμένους προγραμματιστές, ή λόγω έλλειψης προσαρμογής στις αλλαγές στο τοπίο των απειλών, συνήθως χρήση ευάλωτων συστατικών στοιχείων τρίτων ή πλατφορμών χρόνου λειτουργίας.

**ΤΤ4. Αστοχία και διακοπές λειτουργίας**

4.1. *Αστοχία ή δυσλειτουργία εξοπλισμού, διατάξεων ή συστημάτων*

Ως αστοχία ή δυσλειτουργία του εξοπλισμού ορίζεται η ακούσια ζημία σε περιουσιακά στοιχεία ΤΠ λόγω βλάβης ή δυσλειτουργίας του εξοπλισμού, συμπεριλαμβανομένης της υποδομής του παρόχου και των διατάξεων χρήστη.

4.2. *Απώλεια πόρων*

Ως απώλεια πόρων ορίζεται η διακοπή λειτουργίας ή η δυσλειτουργία λόγω μη διαθεσιμότητας τέτοιων πόρων, π.χ. ως εξαρτημάτων συντήρησης.

4.3. *Απώλεια υπηρεσιών υποστήριξης*

Ως απώλεια υπηρεσιών υποστήριξης ορίζεται η διακοπή λειτουργίας ή η δυσλειτουργία λόγω μη διαθεσιμότητας των υπηρεσιών υποστήριξης που απαιτούνται για την ορθή λειτουργία του συστήματος, συμπεριλαμβανομένης της συνδεσιμότητας δικτύου της υποδομής του παρόχου και της διάταξης χρήστη.

**ΤΤ5. Κακόβουλες ενέργειες**

5.1. *Υποκλοπή πληροφοριών*

Ως υποκλοπή πληροφοριών ορίζεται η συλλογή πληροφοριών που δεν προστατεύονται επαρκώς κατά τη διαβίβαση, συμπεριλαμβανομένων των επιθέσεων με τη μέθοδο του «ενδιάμεσου».

5.2. *Ηλεκτρονικό «ψάρεμα» (phishing) και πλαστοπροσωπία (spoofing)*

Ως ηλεκτρονικό «ψάρεμα» ορίζεται η συλλογή πληροφοριών που παρέχει ο χρήστης μετά από παραπλανητική αλληλεπίδραση, η οποία συχνά συνδέεται με την πλαστοπροσωπία (spoofing) στο πλαίσιο νόμιμων μέσων επικοινωνίας και ιστοτόπων. Οι απειλές αυτές στοχεύουν τον χρήστη και συνήθως συντελούν στην Κλοπή ταυτότητας (R4) και στις Μη Εγκεκριμένες συναλλαγές (R9), συχνά μέσω Κλοπής δεδομένων (R5) ή Γνωστοποίησης δεδομένων (R6).

5.3. *Αναπαραγωγή μηνυμάτων*

Ως αναπαραγωγή μηνυμάτων ορίζεται η επαναχρησιμοποίηση μηνυμάτων που έχουν υποκλαπεί προηγουμένως για την εκτέλεση μη εγκεκριμένων συναλλαγών, συχνά σε επίπεδο πρωτοκόλλου. Αυτή η τεχνική απειλή συντελεί κυρίως σε μη εγκεκριμένες συναλλαγές, οι οποίες στη συνέχεια μπορεί να οδηγήσουν σε άλλους κινδύνους, ανάλογα με τη συναλλαγή.

5.4. *Επίθεση ωμής βίας*

Ως επίθεση ωμής βίας ορίζεται η παραβίαση της ασφάλειας, συχνά της εμπιστευτικότητας, με την πραγματοποίηση μεγάλου αριθμού αλληλεπιδράσεων έως ότου οι απαντήσεις παράσχουν πολύτιμες πληροφορίες.

5.5. *Τρωτά σημεία λογισμικού*

Η απειλή που σχετίζεται με τα τρωτά σημεία του λογισμικού συνιστά παραβίαση της ασφάλειας μέσω της εκμετάλλευσης τρωτού σημείου του λογισμικού στα συστατικά στοιχεία του πορτοφολιού ή στα συστατικά στοιχεία λογισμικού και υλισμικού που χρησιμοποιούνται για την υλοποίηση του πορτοφολιού, συμπεριλαμβανομένων των δημοσιευμένων τρωτών σημείων και των μη δημοσιευμένων τρωτών σημείων (μηδενικών ημερών).

5.6. *Επιθέσεις στην αλυσίδα εφοδιασμού*

Ως επίθεση στην αλυσίδα εφοδιασμού ορίζεται η παραβίαση της ασφάλειας μέσω επιθέσεων που διαπράττονται κατά του προμηθευτή του παρόχου πορτοφολιού ή των χρηστών του, ώστε να καταστούν δυνατές περαιτέρω επιθέσεις στο ίδιο το πορτοφόλι.

5.7. *Κακόβουλο λογισμικό*

Ως κακόβουλο λογισμικό ορίζεται η παραβίαση της ασφάλειας μέσω κακόβουλων εφαρμογών που εκτελούν ανεπιθύμητες και παράνομες ενέργειες στο πορτοφόλι.

5.8. *Πρόβλεψη τυχαίων αριθμών*

Ως πρόβλεψη τυχαίων αριθμών ορίζεται η διευκόλυνση επιθέσεων ωμής βίας μέσω μερικής ή πλήρους πρόβλεψης των παραγόμενων τυχαίων αριθμών.

*ΤΜΗΜΑ IV*

***Απειλές για τα πορτοφόλια***

Στην τελευταία αυτήν ενότητα παρουσιάζεται μια επιλογή τυπικών σεναρίων απειλών που αφορούν ειδικά τα πορτοφόλια, τα οποία κατατάσσονται στους βασικούς σχετικούς κινδύνους υψηλού επιπέδου, όπως παρατίθενται ανωτέρω. Ο κατάλογος αυτός υποδεικνύει απειλές που πρέπει να καλυφθούν, αλλά δεν αποτελεί εξαντλητικό κατάλογο απειλών, ο οποίος εξαρτάται σε μεγάλο βαθμό από την αρχιτεκτονική της επιλεγμένης υλοποίησης πορτοφολιού και από την εξέλιξη του περιβάλλοντος των απειλών. Επιπλέον, όσον αφορά την εκτίμηση κινδύνου και τα προτεινόμενα μέτρα, ο πάροχος πορτοφολιού μπορεί να θεωρηθεί υπεύθυνος μόνο για τα συστατικά στοιχεία που εμπίπτουν στο πεδίο εφαρμογής της πιστοποίησης (*).

| ID<br>*Αναγνωριστικό* | Περιγραφή απειλής<br>*Περιγραφή της εντοπισθείσας απειλής* (*) | Τίτλος κινδύνου<br>*Σχετικοί κίνδυνοι* |
|---|---|---|
| TR1 | Ένας επιτιθέμενος μπορεί να ανακαλέσει ψευδώνυμα χωρίς βάσιμο λόγο. | Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR2 | Ένας επιτιθέμενος μπορεί να εκδώσει κατασκευασμένες ηλεκτρονικές ταυτότητες που δεν υπάρχουν. | Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR3 | Ένας επιτιθέμενος μπορεί να αρχίσει να εκδίδει μη εγκεκριμένα δεδομένα ταυτοποίησης προσώπου (PID). | Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR4 | Ένας επιτιθέμενος μπορεί να ζητήσει από έναν διαχειριστή να καταχωρίσει λανθασμένο πάροχο PID στον κατάλογο εμπιστοσύνης παρόχων PID. | Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR5 | Ένας επιτιθέμενος μπορεί να παρακάμψει την υπηρεσία απόδειξης της ταυτότητας εξ αποστάσεως. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR6 | Ένας επιτιθέμενος μπορεί να παρακάμψει την υπηρεσία απόδειξης της ταυτότητας με φυσική παρουσία. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR7 | Ένας επιτιθέμενος μπορεί να παρακάμψει τις υπηρεσίες απόδειξης της ταυτότητας που σχετίζονται με τη χρήση (εγκεκριμένου) πιστοποιητικού εξ αποστάσεως. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR8 | Ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε πορτοφόλι που δεν συνδέεται με κάποιο πρόσωπο. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR9 | Ένας επιτιθέμενος μπορεί να παρακάμψει τους τεχνικούς και διαδικαστικούς ελέγχους για να δημιουργήσει εσφαλμένα PID. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR10 | Ένας επιτιθέμενος μπορεί να ενεργοποιήσει νέο πορτοφόλι σε μη έγκυρη WSCD. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) |
| TR11 | Ένας επιτιθέμενος μπορεί να παρακάμψει την υπηρεσία απόδειξη της ταυτότητας που σχετίζεται με τη χρήση υφιστάμενων μέσων ηλεκτρονικής ταυτοποίησης. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Κλοπή ταυτότητας (R4) / Μη εγκεκριμένη συναλλαγή (R9) |
| TR12 | Ένας επιτιθέμενος μπορεί να παρακάμψει την εκ μέρους του παρόχου PID επαλήθευση του ελέγχου του πορτοφολιού από τον χρήστη και να επιτύχει την έκδοση PID σε παραβιασμένο πορτοφόλι υπό τον έλεγχο του επιτιθέμενου. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Κλοπή ταυτότητας (R4) / Μη εγκεκριμένη συναλλαγή (R9) |

| ID<br>*Αναγνωριστικό* | Περιγραφή απειλής<br>*Περιγραφή της εντοπισθείσας απειλής (*)* | Τίτλος κινδύνου<br>*Σχετικοί κίνδυνοι* |
|---|---|---|
| TR13 | Ένας επιτιθέμενος μπορεί να αποκτήσει έγκυρα PID σε μη έγκυρη μονάδα πορτοφολιού. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Κλοπή ταυτότητας (R4) / Μη εγκεκριμένη συναλλαγή (R9) |
| TR14 | Ένας πάροχος PID μπορεί να εκδώσει κατασκευασμένες ταυτότητες όταν η ταυτότητα σχετίζεται με υφιστάμενο πρόσωπο. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Κλοπή ταυτότητας (R4) / Μη εγκεκριμένη συναλλαγή (R9) |
| TR15 | Ένας επιτιθέμενος μπορεί να συνδέσει μια PID με λανθασμένο πορτοφόλι, επειδή ο πάροχος PID δεν είναι σε θέση να συνδέσει τα PID με το σωστό πορτοφόλι. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Κλοπή ταυτότητας (R4) / Μη εγκεκριμένη συναλλαγή (R9) |
| TR16 | Ένας επιτιθέμενος μπορεί να οδηγήσει τον χρήστη να εγκρίνει την ενεργοποίηση νέας μονάδας/στιγμιότυπου πορτοφολιού υπό τον έλεγχο του επιτιθέμενου —με επακόλουθο έλεγχο και των βεβαιώσεων. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Δημιουργία ή χρήση ψευδούς ηλεκτρονικής ταυτότητας (R2) / Κλοπή ταυτότητας (R4) / Μη εγκεκριμένη συναλλαγή (R9) |
| TR17 | Ένας επιτιθέμενος μπορεί να εκδώσει PID άλλου κράτους για την πρόσβαση σε δεδομένα/ψηφιακά περιουσιακά στοιχεία στοχευόμενων πολιτών. | Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) / Κλοπή ταυτότητας (R4) / Μη εγκεκριμένη συναλλαγή (R9) |
| TR18 | Ένας επιτιθέμενος μπορεί να παρακάμψει τους τεχνικούς και διαδικαστικούς ελέγχους για να δημιουργήσει (εγκεκριμένες) ηλεκτρονικές βεβαιώσεις χαρακτηριστικών [(Q)EAA]. | Δημιουργία ή χρήση ψευδών χαρακτηριστικών (R3) |
| TR19 | Ένας επιτιθέμενος μπορεί να προσκομίσει (Q)EAA που δεν του έχουν χορηγηθεί έγκυρα. | Δημιουργία ή χρήση ψευδών χαρακτηριστικών (R3) |
| TR20 | Ένας επιτιθέμενος μπορεί να επιτεθεί στον μηχανισμό κρυπτογραφικής σύνδεσης του πορτοφολιού μεταξύ των PID και μιας (Q)EAA που δεν θα έπρεπε να τους έχει χορηγηθεί. | Δημιουργία ή χρήση ψευδών χαρακτηριστικών (R3) |
| TR21 | Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει (Q)EAA σε πορτοφόλι, παρόλο που το φυσικό αντίστοιχο της (Q)EAA έχει λήξει ή είναι άκυρο. | Δημιουργία ή χρήση ψευδών χαρακτηριστικών (R3) |
| TR22 | Ένας επιτιθέμενος μπορεί να παρακάμψει την εκ μέρους του παρόχου (Q)EAA επαλήθευση του ελέγχου του πορτοφολιού από τον χρήστη και να επιτύχει την έκδοση (Q)EAA σε παραβιασμένο πορτοφόλι υπό τον έλεγχο του επιτιθέμενου. | Δημιουργία ή χρήση ψευδών χαρακτηριστικών (R3) |
| TR23 | Ένας επιτιθέμενος μπορεί να πλαστογραφήσει ηλεκτρονικές βεβαιώσεις χαρακτηριστικών. | Δημιουργία ή χρήση ψευδών χαρακτηριστικών (R3) |
| TR24 | Ένας επιτιθέμενος μπορεί να εισαγάγει πλαστογραφημένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών σε ένα πορτοφόλι. | Δημιουργία ή χρήση ψευδών χαρακτηριστικών (R3) |
| TR25 | Το πορτοφόλι μπορεί να παρουσιάζει χαρακτηριστικά σε βασιζόμενο μέρος χωρίς την έγκριση του χρήστη. | Γνωστοποίηση δεδομένων (R6) |
| TR26 | PID, (Q)EAA ή ψευδώνυμα μπορούν να παρουσιαστούν σε εσφαλμένο βασιζόμενο μέρος. | Γνωστοποίηση δεδομένων (R6) |
| TR27 | Ένας επιτιθέμενος μπορεί να κινήσει κακόβουλη ανανέωση EAA. | Γνωστοποίηση δεδομένων (R6) |
| TR28 | Ένας επιτιθέμενος μπορεί να οδηγήσει έναν χρήστη να εγκρίνει εσφαλμένα αίτημα έκδοσης ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (ηλεκτρονικό «ψάρεμα» ή άλλο). | Γνωστοποίηση δεδομένων (R6) |

| ID<br>*Αναγνωριστικό* | Περιγραφή απειλής<br>*Περιγραφή της εντοπισθείσας απειλής (*)* | Τίτλος κινδύνου<br>*Σχετικοί κίνδυνοι* |
|---|---|---|
| TR29 | Ένας επιτιθέμενος μπορεί να διαρρεύσει χαρακτηριστικά από το πορτοφόλι και να ταυτοποιήσει τον χρήστη πορτοφολιού όταν η ταυτοποίηση δεν απαιτείται / δεν επιτρέπεται. | Γνωστοποίηση δεδομένων (R6) |
| TR30 | Ένας επιτιθέμενος μπορεί να παρακάμψει τους τεχνικούς και διαδικαστικούς ελέγχους για να εξαγάγει δεδομένα. | Γνωστοποίηση δεδομένων (R6) |
| TR31 | Ένα αίτημα μπορεί να διαρρεύσει σε επιτιθέμενο. | Γνωστοποίηση δεδομένων (R6) |
| TR32 | Ένας επιτιθέμενος μπορεί να λάβει γνώση της ενσωματωμένης πολιτικής γνωστοποίησης χαρακτηριστικών και να παρουσιάσει χαρακτηριστικά που περιέχονται στο τρέχον αίτημα από μονάδες πορτοφολιού. | Γνωστοποίηση δεδομένων (R6) |
| TR33 | Ένας επιτιθέμενος μπορεί να εξαγάγει αρχεία καταγραφής ή μέρη αυτών. | Γνωστοποίηση δεδομένων (R6) |
| TR34 | Ένας επιτιθέμενος μπορεί να γνωρίζει αν ένα πορτοφόλι είναι εγκατεστημένο στην ίδια διάταξη την οποία χρησιμοποιεί ή σε άλλη διάταξη και να αποκτήσει πληροφορίες σχετικά με αυτό. | Γνωστοποίηση δεδομένων (R6) |
| TR35 | Ένας επιτιθέμενος μπορεί να αποκτήσει έναν παράγοντα γνώσης που χρησιμοποιείται για την επαλήθευση της ταυτότητας χρηστών στην WSCA. | Γνωστοποίηση δεδομένων (R6) |
| TR36 | Η ηλεκτρονική βεβαίωση χαρακτηριστικών σχετικά με ένα πρόσωπο που προσκομίζεται σε πολλαπλές συναλλαγές με βασιζόμενο μέρος ή μεταξύ διαφορετικών βασιζόμενων μερών επιτρέπει ακούσια τη σύνδεση πολλαπλών συναλλαγών με το σχετικό πρόσωπο. | Γνωστοποίηση δεδομένων (R6) |
| TR37 | Ένας δημόσιος κατάλογος ανάκλησης βεβαιώσεων/βασιζόμενων μερών μπορεί να περιέχει πληροφορίες σχετικά με τη χρήση της βεβαίωσης από τον χρήστη (π.χ. θέση, διεύθυνση IP...). | Γνωστοποίηση δεδομένων (R6) |
| TR38 | Δεδομένου ότι δεν είναι σε θέση να αποδείξουν τη συγκατάθεση του χρήστη για τον διαμοιρασμό χαρακτηριστικών, τα βασιζόμενα μέρη μπορούν να επηρεάσουν την ακεραιότητα των αρχείων καταγραφής. | Γνωστοποίηση δεδομένων (R6) |
| TR39 | Ένας επιτιθέμενος μπορεί να εντοπίσει παράνομα χρήστες πορτοφολιού χρησιμοποιώντας μοναδικά/ανιχνεύσιμα αναγνωριστικά. | Γνωστοποίηση δεδομένων (R6) / Εποπτεία (R14) |
| TR40 | Ένα βασιζόμενο μέρος που αποτελείται από πολλαπλές μονάδες/οντότητες καθεμία από τις οποίες έχει διαφορετικό πεδίο εφαρμογής από αυτό που επιτρέπεται να ζητήσει/να επεξεργαστεί, μπορεί να ζητήσει και να επεξεργαστεί δεδομένα για τα οποία δεν έχει νόμιμους λόγους. | Γνωστοποίηση δεδομένων (R6) / Μη εγκεκριμένη συναλλαγή (R9) |
| TR41 | Ένας επιτιθέμενος μπορεί να υπονομεύσει τους ελέγχους ακεραιότητας και γνησιότητας των PID που διενεργεί το πορτοφόλι ώστε οι έλεγχοι να έχουν πάντα επιτυχή έκβαση. | Παραποίηση δεδομένων (R7) |
| TR42 | Ένας επιτιθέμενος μπορεί να παρακάμψει ή να υπονομεύσει την εκ μέρους του πορτοφολιού διενέργεια ελέγχων οι οποίοι επαληθεύουν την ακεραιότητα και τη γνησιότητα των ζητούμενων χαρακτηριστικών, ώστε οι έλεγχοι να έχουν πάντα επιτυχή έκβαση. | Παραποίηση δεδομένων (R7) |
| TR43 | Ένας επιτιθέμενος μπορεί να παρακάμψει ή να υπονομεύσει την εκ μέρους του πορτοφολιού διενέργεια ελέγχων οι οποίοι επαληθεύουν ότι όλα τα ζητούμενα χαρακτηριστικά ανήκουν στον ίδιο χρήστη, ώστε οι έλεγχοι να έχουν πάντα επιτυχή έκβαση. | Παραποίηση δεδομένων (R7) |
| TR44 | Ένας επιτιθέμενος μπορεί να παρακάμψει ή να υπονομεύσει την εκ μέρους του πορτοφολιού διενέργεια ελέγχων οι οποίοι επαληθεύουν ότι τα PID είναι έγκυρα και έχουν εκδοθεί από αξιόπιστο πάροχο PID, ώστε οι έλεγχοι να έχουν πάντα επιτυχή έκβαση. | Παραποίηση δεδομένων (R7) |

| ID<br>*Αναγνωριστικό* | Περιγραφή απειλής<br>*Περιγραφή της εντοπισθείσας απειλής (*)* | Τίτλος κινδύνου<br>*Σχετικοί κίνδυνοι* |
|---|---|---|
| TR45 | Ένας επιτιθέμενος μπορεί να παρακάμψει ή να υπονομεύσει την εκ μέρους του πορτοφολιού διενέργεια ελέγχων οι οποίοι επαληθεύουν ότι μια QEAA είναι έγκυρη και έχει εκδοθεί από αναγνωρισμένο πάροχο τεχνικών υπηρεσιών, ο οποίος είναι εγγεγραμμένος για την έκδοση της QEAA, ώστε οι έλεγχοι να έχουν πάντα επιτυχή έκβαση. | Παραποίηση δεδομένων (R7) |
| TR46 | Ένας επιτιθέμενος μπορεί να παρακάμψει ή να υπονομεύσει την εκ μέρους του πορτοφολιού διενέργεια ελέγχων οι οποίοι επαληθεύουν αν τα PID έχουν ανακληθεί από τον πάροχο PID, ώστε οι έλεγχοι να έχουν πάντα επιτυχή έκβαση. | Παραποίηση δεδομένων (R7) |
| TR47 | Ένας επιτιθέμενος μπορεί να παρακάμψει ή να υπονομεύσει την εκ μέρους του πορτοφολιού διενέργεια ελέγχων οι οποίοι επαληθεύουν αν η (Q)EAA έχει ανακληθεί από τον πάροχο (Q) EAA, ώστε οι έλεγχοι να έχουν πάντα επιτυχή έκβαση. | Παραποίηση δεδομένων (R7) |
| TR48 | Ένας επιτιθέμενος μπορεί να τροποποιήσει το περιεχόμενο των δεδομένων αντιγράφων ασφαλείας και των δεδομένων ανάκτησης που θα πρέπει να τελούν αποκλειστικά υπό τον έλεγχο του χρήστη. | Παραποίηση δεδομένων (R7) / Απώλεια δεδομένων (R8) |
| TR49 | Ένας επιτιθέμενος μπορεί να τροποποιήσει το ιστορικό συναλλαγών για ένα δεδομένο στιγμιότυπο πορτοφολιού από τα αρχεία καταγραφής δραστηριοτήτων. | Παραποίηση δεδομένων (R7) / Απώλεια δεδομένων (R8) |
| TR50 | Ένας επιτιθέμενος μπορεί να προβεί σε λαθραχρόαση κατά τη διάρκεια της σύνδεσης από το πορτοφόλι με βασιζόμενα μέρη. | Κλοπή δεδομένων (R5) / Γνωστοποίηση δεδομένων (R6) |
| TR51 | Ένας επιτιθέμενος μπορεί να πείσει έναν χρήστη να κοινοποιήσει δεδομένα προσωπικού χαρακτήρα (π.χ. PID, EAA, ψευδώνυμα, ηλεκτρονικές υπογραφές, αρχεία καταγραφής και άλλα δεδομένα) στον επιτιθέμενο ή σε τρίτο, κάτι που ο χρήστης δεν είχε πρόθεση να πράξει. | Κλοπή δεδομένων (R5) / Γνωστοποίηση δεδομένων (R6) |
| TR52 | Ένας επιτιθέμενος μπορεί να διαβάσει το ιστορικό συναλλαγών για ένα συγκεκριμένο στιγμιότυπο πορτοφολιού από τα αρχεία καταγραφής δραστηριοτήτων. | Κλοπή δεδομένων (R5) / Γνωστοποίηση δεδομένων (R6) |
| TR53 | Ένας επιτιθέμενος μπορεί να εξαγάγει ή να αντλήσει υλικό κρυπτογραφικών κλειδιών εκτός της WSCD. | Κλοπή δεδομένων (R5) / Γνωστοποίηση δεδομένων (R6) / Μη εγκεκριμένη συναλλαγή (R9) |
| TR54 | Ένας επιτιθέμενος μπορεί να αναγνώσει το περιεχόμενο των δεδομένων αντιγράφων ασφαλείας και των δεδομένων ανάκτησης που θα πρέπει να τελούν αποκλειστικά υπό τον έλεγχο του χρήστη. | Κλοπή δεδομένων (R5) / Γνωστοποίηση δεδομένων (R6) |
| TR55 | Ένας επιτιθέμενος μπορεί να παρακάμψει τη μέθοδο επαλήθευσης ταυτότητας χρήστη για να χρησιμοποιήσει ψευδώνυμο που δημιουργείται από μονάδα πορτοφολιού. | Κλοπή ταυτότητας (R4) |
| TR56 | Ένας επιτιθέμενος μπορεί να προτείνει στους χρήστες μια εφαρμογή που μιμείται ένα συγκεκριμένο νόμιμο πορτοφόλι. | Κλοπή ταυτότητας (R4) |
| TR57 | Ένας επιτιθέμενος μπορεί να εξαγάγει δεδομένα πορτοφολιού, συμπεριλαμβανομένων PID, (Q)EAA ή αρχείων καταγραφής. | Κλοπή ταυτότητας (R4) |
| TR58 | Ένας επιτιθέμενος μπορεί να εξαγάγει κρυπτογραφικό συνδετικό υλικό. | Κλοπή ταυτότητας (R4) |
| TR59 | Ένας επιτιθέμενος μπορεί να αναλάβει ταυτότητες μέσω των κρυπτογραφικών κλειδιών του πορτοφολιού. | Κλοπή ταυτότητας (R4) |
| TR60 | Ένας επιτιθέμενος μπορεί να αναπαραγάγει τη μονάδα προσωπικού πορτοφολιού άλλου χρήστη στην προσωπική του διάταξη και να τη χρησιμοποιήσει. | Κλοπή ταυτότητας (R4) / Δημιουργία ή χρήση υφιστάμενης ηλεκτρονικής ταυτότητας (R1) |

| ID<br>*Αναγνωριστικό* | Περιγραφή απειλής<br>*Περιγραφή της εντοπισθείσας απειλής (*)* | Τίτλος κινδύνου<br>*Σχετικοί κίνδυνοι* |
|---|---|---|
| TR61 | Οι αρχές άλλου κράτους μπορούν να ζητήσουν από τον χρήστη να επιδείξει και/ή να κοινοποιήσει όλα τα δεδομένα πορτοφολιού σε κατάσταση εγγύτητας, όπως κατά τη διέλευση των συνόρων του εν λόγω κράτους. | Κλοπή ταυτότητας (R4) / Εποπτεία (R14) |
| TR62 | Οι χρήστες δεν μπορούν να μεταφέρουν τα αρχεία καταγραφής συναλλαγών τους μετά από αστοχία διάταξης χρήστη, κάτι που έχει ως αποτέλεσμα την απώλεια της ιχνηλασιμότητας προηγούμενων συναλλαγών στο νέο πορτοφόλι. | Αποκήρυξη (R11) |
| TR63 | Οι χρήστες δεν μπορούν να ανακτήσουν τα αρχεία καταγραφής συναλλαγών τους μετά από αστοχία διάταξης χρήστη, κάτι που έχει ως αποτέλεσμα την απώλεια της ιχνηλασιμότητας στο νέο πορτοφόλι. | Αποκήρυξη (R11) |
| TR64 | Τα βασιζόμενα μέρη ενδέχεται να δυσκολεύονται να αποδείξουν τη συγκατάθεσή τους για εξ αποστάσεως ηλεκτρονικές υπογραφές. | Αποκήρυξη (R11) |
| TR65 | Ένας επιτιθέμενος μπορεί να κατακλύσει τη σύνδεση ή τις συνδέσεις με αιτήματα κατά τη διάρκεια της σύνδεσης με τα βασιζόμενα μέρη. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR66 | Ένας επιτιθέμενος μπορεί να κατακλύσει μια υπηρεσία παροχής καθεστώτος με συνδέσεις με βασιζόμενα μέρη. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR67 | Ένας επιτιθέμενος μπορεί να κάνει την προσκόμιση του χαρακτηριστικού να φαίνεται ως αμφισβητούμενη/απορριφθείσα, παρότι η προσκόμιση του χαρακτηριστικού δηλώνει την εγκυρότητά του. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR68 | Ένας επιτιθέμενος μπορεί να ανακαλέσει PID χωρίς βάσιμο λόγο. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR69 | Ένας επιτιθέμενος μπορεί να ανακαλέσει PID χωρίς τη συγκατάθεση του χρήστη. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR70 | Ένας επιτιθέμενος μπορεί να ανακαλέσει (Q)EAA χωρίς βάσιμο λόγο. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR71 | Ένας επιτιθέμενος μπορεί να ανακαλέσει (Q)EAA χωρίς τη συγκατάθεση του χρήστη. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR72 | Ένας επιτιθέμενος μπορεί να υποβάλει πολλαπλά αιτήματα ταυτοποίησης χωρίς αυτά να αναγνωρίζονται ως σκόπιμα ορφανά αιτήματα. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR73 | Ένας επιτιθέμενος μπορεί να αποστείλει πολλαπλά αιτήματα χωρίς επακόλουθη συναλλαγή. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR74 | Ένας επιτιθέμενος μπορεί να επιτρέψει σε βασιζόμενο μέρος να ζητήσει ταυτοποίηση χωρίς αντίστοιχο αναγνωριστικό (απάντηση) και πλήρη έλεγχο. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR75 | Ένας επιτιθέμενος μπορεί να αποστείλει απάντηση σε αίτημα μετά τη λήξη της προθεσμίας, ή σε παρόμοιες καταστάσεις που οδηγούν σε διαταραχή της παροχής υπηρεσίας. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR76 | Ένα βασιζόμενο μέρος μπορεί να αποστείλει πολλαπλά μη έγκυρα αιτήματα. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR77 | Ένας επιτιθέμενος μπορεί να αποστείλει πολλαπλά μη έγκυρα αιτήματα σε πάροχο πορτοφολιού. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR78 | Ένας επιτιθέμενος μπορεί να καταστήσει ένα κράτος μέλος ανίκανο να ανακαλέσει έναν μη αξιόπιστο πάροχο PID από τον κατάλογο εμπιστοσύνης αξιόπιστων παρόχων PID. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR79 | Ένας επιτιθέμενος μπορεί να αποτρέψει την αναστολή ή την ανάκληση πορτοφολιού. | Διαταραχή στην παροχή υπηρεσίας (R13) |

| ID<br>*Αναγνωριστικό* | Περιγραφή απειλής<br>*Περιγραφή της εντοπισθείσας απειλής (*)* | Τίτλος κινδύνου<br>*Σχετικοί κίνδυνοι* |
|---|---|---|
| TR80 | Ένας επιτιθέμενος μπορεί να εμποδίσει συναλλαγές βασιζόμενων μερών, χρηστών και/ή παρόχου PID. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR81 | Ένας επιτιθέμενος μπορεί να απενεργοποιήσει ή να καταστήσει μη διαθέσιμη την WSCD. | Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR82 | Ένας επιτιθέμενος μπορεί να καταστήσει τον πάροχο PID ανίκανο να ανακαλέσει ή να αναστείλει PID. | Διαταραχή στην παροχή υπηρεσίας (R13) / Μη εγκεκριμένη συναλλαγή (R9) |
| TR83 | Ένα βασιζόμενο μέρος μπορεί να αντλήσει τα δεδομένα ταυτότητας του χρήστη πέραν των δεδομένων που του κοινοποιούνται. | Εποπτεία (R14) |
| TR84 | Μια ομάδα συνεργαζόμενων βασιζόμενων μερών ή παρόχων PID μπορούν να αντλήσουν τα δεδομένα ταυτότητας του χρήστη πέραν των δεδομένων που είναι γνωστά σε αυτούς. | Εποπτεία (R14) |
| TR85 | Ένας επιτιθέμενος μπορεί να παρακολουθεί και να εντοπίζει έναν χρήστη χρησιμοποιώντας τα δεδομένα ταυτοποίησης προσώπου του χρήστη, όταν δεν απαιτείται ταυτοποίηση του χρήστη. | Εποπτεία (R14) |
| TR86 | Ένας επιτιθέμενος μπορεί να συνδυάσει μια παραποιημένη παρουσίαση συνδυασμών (Q)EAA. | Παραποίηση συναλλαγών (R10) |
| TR87 | Ένας επιτιθέμενος μπορεί να ενεργοποιήσει/αναλάβει εξ αποστάσεως το πορτοφόλι (π.χ. τραπεζική εφαρμογή που ενσωματώνει αίτημα επαλήθευσης ταυτότητας ή βεβαίωσης) χωρίς τη ρητή συγκατάθεση ή τον αποκλειστικό έλεγχο του χρήστη, σε περιπτώσεις κατά τις οποίες ο χρήστης δεν έχει επίγνωση (π.χ. κοιμάται) ή δεν μπορεί να δει το βασιζόμενο μέρος. | Παραποίηση συναλλαγών (R10) |
| TR88 | Οι επιτιθέμενοι μπορούν να επιφέρουν αλλαγές στα μεταδεδομένα ενός αιτήματος (όνομα υπηρεσίας, χρήσεις κ.λπ.). | Παραποίηση συναλλαγών (R10) |
| TR89 | Οι επιτιθέμενοι μπορούν να προβούν σε αλλαγές στις πληροφορίες αντίδρασης [κατάσταση υπηρεσίας, μοναδικός αριθμός (nonce) κ.λπ.]. | Παραποίηση συναλλαγών (R10) |
| TR90 | Οι επιτιθέμενοι μπορούν να επιφέρουν αλλαγές στις πληροφορίες σχετικά με τα χαρακτηριστικά ενός αιτήματος (διατύπωση υπερβολικών ερωτημάτων κ.λπ.). | Παραποίηση συναλλαγών (R10) |
| TR91 | Ένα βασιζόμενο μέρος μπορεί να αναπαραγάγει στοιχεία από προηγούμενη περίοδο λειτουργίας σε άλλη περίοδο λειτουργίας. | Παραποίηση συναλλαγών (R10) |
| TR92 | Ένας επιτιθέμενος μπορεί να αντικαταστήσει ή να τροποποιήσει τα PID κατά τη μεταφορά τους από τον πάροχο PID στη μονάδα πορτοφολιού. | Παραποίηση συναλλαγών (R10) |
| TR93 | Ένας επιτιθέμενος μπορεί να αντικαταστήσει ή να τροποποιήσει τα PID κατά τη μεταφορά τους από τη μονάδα πορτοφολιού στο βασιζόμενο μέρος στο διαδίκτυο. | Παραποίηση συναλλαγών (R10) |
| TR94 | Ένας επιτιθέμενος μπορεί να αντικαταστήσει ή να τροποποιήσει τα PID κατά τη μεταφορά τους από τη μονάδα πορτοφολιού στο βασιζόμενο μέρος εκτός διαδικτύου. | Παραποίηση συναλλαγών (R10) |
| TR95 | Ένας επιτιθέμενος μπορεί να εκδώσει PID χωρίς τη συγκατάθεση του χρήστη. | Μη εγκεκριμένη συναλλαγή (R9) |
| TR96 | Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει ανακληθείσες ή μη έγκυρες ενσωματωμένες πολιτικές γνωστοποίησης, ενδεχομένως εν αγνοία των βασιζόμενων μερών. | Μη εγκεκριμένη συναλλαγή (R9) |
| TR97 | Ένας επιτιθέμενος μπορεί να ξεγελάσει το πορτοφόλι ώστε να επαληθεύσει εσφαλμένες ηλεκτρονικές υπογραφές. | Μη εγκεκριμένη συναλλαγή (R9) |
| TR98 | Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει το πορτοφόλι εκτός του ελέγχου του χρήστη. | Μη εγκεκριμένη συναλλαγή (R9) |

| ID<br>*Αναγνωριστικό* | Περιγραφή απειλής<br>*Περιγραφή της εντοπισθείσας απειλής (*)* | Τίτλος κινδύνου<br>*Σχετικοί κίνδυνοι* |
|---|---|---|
| TR99 | Ένας επιτιθέμενος μπορεί να πείσει τον χρήστη να επαληθεύσει την ταυτότητα και να εγκρίνει συναλλαγές με επιτιθέμενο ή μη εξουσιοδοτημένο τρίτο. | Μη εγκεκριμένη συναλλαγή (R9) |
| TR100 | Ένας επιτιθέμενος μπορεί να πείσει τον χρήστη να τοποθετήσει ηλεκτρονική υπογραφή χωρίς να παρουσιάσει το περιεχόμενο στον χρήστη ή μετά την παρουσίαση εσφαλμένου περιεχομένου. | Μη εγκεκριμένη συναλλαγή (R9) |
| TR101 | Ένας επιτιθέμενος μπορεί να παρακάμψει τον έλεγχο πρόσβασης του λογαριασμού του χρήστη στον πάροχο πορτοφολιού. | Μη εγκεκριμένη συναλλαγή (R9) |
| TR102 | Ένας επιτιθέμενος μπορεί να υποκλέψει την ταυτότητα των βασιζόμενων μερών κατά τη διάρκεια της σύνδεσης με τα βασιζόμενα μέρη. | Μη εγκεκριμένη συναλλαγή (R9) / Γνωστοποίηση δεδομένων (R6) |
| TR103 | Ο χρήστης πίσω από τη σύνδεση μεταξύ βασιζόμενου μέρους και φυλλομετρητή μπορεί να διαφέρει από τον χρήστη πίσω από τη σύνδεση μεταξύ βασιζόμενου μέρους και πορτοφολιού. | Μη εγκεκριμένη συναλλαγή (R9) / Γνωστοποίηση δεδομένων (R6) / Κλοπή ταυτότητας (R4) |
| TR104 | Ένας επιτιθέμενος μπορεί να πείσει τον χρήστη να ανακαλέσει το πορτοφόλι του χρήστη χωρίς λόγο. | Μη εγκεκριμένη συναλλαγή (R9) / Διαταραχή στην παροχή υπηρεσίας (R13) |
| TR105 | Ένας επιτιθέμενος μπορεί να προβεί σε επιθέσεις με τη μέθοδο του «ενδιάμεσου». | Μη εγκεκριμένη συναλλαγή (R9) / Γνωστοποίηση δεδομένων (R6) / Εποπτεία (R14) |
| TR106 | Ένας επιτιθέμενος μπορεί να παρουσιάσει μη έγκυρα ή ανακληθέντα χαρακτηριστικά από πορτοφόλι που δεν συνδέεται τακτικά με το δίκτυο. | Επιπτώσεις στους διάφορους κινδύνους |
| TR107 | Ένας επιτιθέμενος μπορεί να κλέψει πληροφορίες από έναν χρήστη χρησιμοποιώντας ένα παραπλανητικό πορτοφόλι. | Επιπτώσεις στους διάφορους κινδύνους |
| TR108 | Ένας επιτιθέμενος μπορεί να προσποιηθεί τον χρήστη αναπαράγοντας/μιμούμενος ένα αίτημα δεδομένων (π.χ. επαλήθευση ταυτότητας), το οποίο θα φαίνεται ως έγκυρο. | Επιπτώσεις στους διάφορους κινδύνους |
| TR109 | Ένας επιτιθέμενος μπορεί να αναπαραγάγει μια ενσωματωμένη πολιτική γνωστοποίησης προς έναν χρήστη, για να μιμηθεί ένα εγκεκριμένο αίτημα. | Επιπτώσεις στους διάφορους κινδύνους |
| TR110 | Ένας επιτιθέμενος μπορεί να εκμεταλλευθεί την έλλειψη πληροφοριών των χρηστών πορτοφολιού, ή αδικαιολόγητες καθυστερήσεις, μετά από παραβίαση της ασφάλειας ή έκθεση σε κίνδυνο. | Επιπτώσεις στους διάφορους κινδύνους |
| TR111 | Ένας επιτιθέμενος μπορεί να τροποποιήσει ένα παλαιότερα εγκατεστημένο νόμιμο στιγμιότυπο πορτοφολιού για να προσθέσει κακόβουλα χαρακτηριστικά. | Επιπτώσεις στους διάφορους κινδύνους |
| TR112 | Ένας επιτιθέμενος μπορεί να τροποποιήσει ένα νόμιμο στιγμιότυπο πορτοφολιού και να το προτείνει στους χρήστες ως νόμιμο. | Επιπτώσεις στους διάφορους κινδύνους |
| TR113 | Ένας επιτιθέμενος μπορεί να καταστείλει τον ίδιο τον μηχανισμό επαλήθευσης ταυτότητας χρήστη για να παρακάμψει την επαλήθευση ταυτότητας του χρήστη πορτοφολιού. | Επιπτώσεις στους διάφορους κινδύνους |
| TR114 | Ένας επιτιθέμενος μπορεί να εισαγάγει κακόβουλο κωδικό ή κερκόπορτες στον κώδικα πορτοφολιού κατά την ανάπτυξή του στη διάταξη χρήστη. | Επιπτώσεις στους διάφορους κινδύνους |
| TR115 | Ένας επιτιθέμενος μπορεί να εισαγάγει κακόβουλο κωδικό ή κερκόπορτες στον κώδικα πορτοφολιού κατά τη διάρκεια της ανάπτυξής του. | Επιπτώσεις στους διάφορους κινδύνους |
| TR116 | Ένας επιτιθέμενος μπορεί να παραποιήσει τη δημιουργία τυχαίων αριθμών ώστε να μειωθεί επαρκώς η εντροπία τους και να είναι δυνατές οι επιθέσεις. | Επιπτώσεις στους διάφορους κινδύνους |

| ID<br>*Αναγνωριστικό* | Περιγραφή απειλής<br>*Περιγραφή της εντοπισθείσας απειλής (*)* | Τίτλος κινδύνου<br>*Σχετικοί κίνδυνοι* |
|---|---|---|
| TR117 | Ένας επιτιθέμενος μπορεί να παραποιήσει τις διατάξεις χρήστη στην αλυσίδα εφοδιασμού για να συμπεριλάβει κώδικα ή διαμορφώσεις που δεν πληρούν τις προϋποθέσεις χρήσης του πορτοφολιού. | Επιπτώσεις στους διάφορους κινδύνους |
| TR118 | Ένας επιτιθέμενος μπορεί να ενεργοποιήσει μια μονάδα πορτοφολιού χρησιμοποιώντας παραποιημένη WSCD που ελέγχεται από τους επιτιθέμενους. | Επιπτώσεις στους διάφορους κινδύνους |
| TR119 | Ένας επιτιθέμενος μπορεί να διαβάσει τις πληροφορίες που αποστέλλονται στην WSCA και/ή στην WSCD. | Επιπτώσεις στους διάφορους κινδύνους |
| TR120 | Ένας επιτιθέμενος μπορεί να αποστείλει αυθαίρετες πληροφορίες στην WSCA. | Επιπτώσεις στους διάφορους κινδύνους |
| TR121 | Ένας επιτιθέμενος μπορεί να κλέψει πληροφορίες παρακολουθώντας τις ανταλλαγές μεταξύ της WSCA και της WSCD. | Επιπτώσεις στους διάφορους κινδύνους |
| TR122 | Ένας επιτιθέμενος μπορεί να αποστείλει αυθαίρετες πληροφορίες στην WSCD. | Επιπτώσεις στους διάφορους κινδύνους |
| TR123 | Ένας επιτιθέμενος μπορεί να αποστείλει πληροφορίες στην WSCD, παρακάμπτοντας την WSCA. | Επιπτώσεις στους διάφορους κινδύνους |
| TR124 | Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει ηλεκτρονικό «ψάρεμα» για να προσελκύσει χρήστες σε πλαστή διαδικτυακή εφαρμογή διαχείρισης πλαστών πορτοφολιών και PID. | Επιπτώσεις στους διάφορους κινδύνους |
| TR125 | Ένας επιτιθέμενος μπορεί να αντικαταστήσει τα κλειδιά ενός πορτοφολιού με άλλα κλειδιά για τη δημιουργία μηνυμάτων που θα χρησιμοποιηθούν σε άλλη επίθεση. | Επιπτώσεις στους διάφορους κινδύνους |
| TR126 | Ένας επιτιθέμενος μπορεί να τροποποιήσει ή να καταστρέψει τα κλειδιά ενός πορτοφολιού, καθιστώντας μη χρησιμοποιήσιμες ορισμένες λειτουργίες του πορτοφολιού. | Επιπτώσεις στους διάφορους κινδύνους |
| TR127 | Ένας επιτιθέμενος μπορεί να ελέγχει κακόβουλο λογισμικό για την πρόσβαση σε δεδομένα που είναι αποθηκευμένα στο πορτοφόλι. | Επιπτώσεις στους διάφορους κινδύνους |
| TR128 | Ένας επιτιθέμενος μπορεί να έχει πρόσβαση σε αποδεικτικά στοιχεία που παράγονται στο πορτοφόλι. | Επιπτώσεις στους διάφορους κινδύνους |
| TR129 | Οι πάροχοι πορτοφολιού μπορούν να έχουν πρόσβαση σε αντικείμενα στο πορτοφόλι. | Επιπτώσεις στους διάφορους κινδύνους |
| TR130 | Οι πάροχοι πορτοφολιών μπορούν να έχουν πρόσβαση σε αποδεικτικά στοιχεία που παράγονται στο πορτοφόλι. | Επιπτώσεις στους διάφορους κινδύνους |
| TR131 | Ένας επιτιθέμενος μπορεί να κλέψει μια μη κλειδωμένη διάταξη πορτοφολιού. | Επιπτώσεις στους διάφορους κινδύνους |
| TR132 | Ένας επιτιθέμενος μπορεί να χειραγωγήσει το σύστημα ώστε να αποτρέψει την καταγραφή ορισμένων συμβάντων. | Επιπτώσεις στους διάφορους κινδύνους |
| TR133 | Ένας επιτιθέμενος μπορεί να παρακολουθήσει την επικοινωνία μεταξύ του στιγμιότυπου πορτοφολιού και της WSCA ή να αναπαραγάγει/μιμηθεί έναν χρήστη (π.χ. με πειρατεία μηχανισμού επαλήθευσης ταυτότητας). | Επιπτώσεις στους διάφορους κινδύνους |

*ΠΑΡΑΡΤΗΜΑ II*

**ΚΡΙΤΗΡΙΑ ΓΙΑ ΤΗΝ ΑΞΙΟΛΟΓΗΣΗ ΤΗΣ ΑΠΟΔΟΧΗΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΔΙΑΣΦΑΛΙΣΗΣ**

| Όνομα | Αντικείμενο | Σημεία στα οποία πρέπει να δοθεί προσοχή |
|---|---|---|
| EUCC | Προϊόντα ΤΠΕ | Σχετικά με τον εκδότη: ουδέν (διαπιστευμένοι οργανισμοί πιστοποίησης)<br>Σχετικά με το πεδίο εφαρμογής:<br>— Ελέγξτε το προφίλ προστασίας και τον στόχο ασφάλειας<br>— Ελέγξτε το επίπεδο διασφάλισης και τις επεκτάσεις της αξιολόγησης<br>Σχετικά με τη διασφάλιση:<br>— Ελέγξτε τους περιορισμούς στην τεκμηρίωση χρήστη<br>— Όσον αφορά τη σύνθεση, μπορεί να απαιτηθεί πρόσβαση στην τεχνική έκθεση αξιολόγησης |
| EUCS (εφόσον υπάρχει) | Υπηρεσίες υπολογιστικού νέφους | Σχετικά με τον εκδότη: ουδέν (διαπιστευμένοι οργανισμοί πιστοποίησης)<br>Σχετικά με το πεδίο εφαρμογής:<br>— Ελέγξτε την περιγραφή της υπηρεσίας υπολογιστικού νέφους<br>— Ελέγξτε το επίπεδο αξιολόγησης και τα προφίλ επέκτασης<br>Σχετικά με τη διασφάλιση:<br>— Ελέγξτε τις πληροφορίες σχετικά με τη διαφάνεια και, εάν χρειάζεται, τις πληροφορίες σχετικά με τη σύνθεση |
| Σχήματα Κοινών Κριτηρίων που λειτουργούν στην ΕΕ, συμπεριλαμβανομένων των σχημάτων SOG-IS | Προϊόντα ΤΠΕ | Σχετικά με τον εκδότη: ουδέν (κράτη μέλη)<br>Σχετικά με το πεδίο εφαρμογής:<br>— Ελέγξτε το προφίλ προστασίας και τον στόχο ασφάλειας<br>— Ελέγξτε το επίπεδο διασφάλισης και τις επεκτάσεις της αξιολόγησης<br>Σχετικά με τη διασφάλιση:<br>— Ελέγξτε τους περιορισμούς στην τεκμηρίωση χρήστη<br>— Όσον αφορά τη σύνθεση, μπορεί να απαιτηθεί πρόσβαση στην τεχνική έκθεση αξιολόγησης |
| EN 17640:2018 (FITCEM, συμπεριλαμβανομένων των CSPN, BSZ, LINCE, BSZA) | Προϊόντα ΤΠΕ | Σχετικά με τον εκδότη:<br>— Ελέγξτε το σχήμα και τις απαιτήσεις για τους οργανισμούς πιστοποίησης<br>Σχετικά με το πεδίο εφαρμογής:<br>— Ελέγξτε την περιγραφή του προϊόντος<br>— Ελέγξτε τους ισχυρισμούς περί ασφάλειας<br>— Ελέγξτε το επίπεδο διασφάλισης<br>Σχετικά με τη διασφάλιση:<br>— Ελέγξτε τις δραστηριότητες που εκτελέστηκαν και τα πορίσματα της έκθεσης |
| Σχήματα πιστοποίησης εγκεκριμένων διατάξεων δημιουργίας υπογραφής σύμφωνα με το άρθρο 30 του κανονισμού (ΕΕ) αριθ. 910/2014 | QSCD | Σχετικά με τον εκδότη:<br>— Ελέγξτε το σχήμα και τις απαιτήσεις για τους οργανισμούς πιστοποίησης<br>Σχετικά με το πεδίο εφαρμογής:<br>— Ελέγξτε την περιγραφή του προϊόντος<br>— Ελέγξτε τους ισχυρισμούς περί ασφάλειας<br>— Ελέγξτε το επίπεδο διασφάλισης<br>Σχετικά με τη διασφάλιση:<br>— Ελέγξτε τις δραστηριότητες που εκτελέστηκαν |

| Όνομα | Αντικείμενο | Σημεία στα οποία πρέπει να δοθεί προσοχή |
|---|---|---|
| EN ISO/IEC 27001:2022 | ISMS | Σχετικά με τον εκδότη: κανένας (διαπιστευμένοι οργανισμοί πιστοποίησης)<br>Σχετικά με το πεδίο εφαρμογής:<br>— Ελέγξτε την περιγραφή του συστήματος διαχείρισης<br>— Ελέγξτε τη δήλωση εφαρμογής<br>Σχετικά με τη διασφάλιση:<br>— Ελέγξτε τις δραστηριότητες που εκτελέστηκαν |
| SOC2 | Οργανισμοί | Σχετικά με τον εκδότη:<br>— Ελέγξτε το καθεστώς του ως λογιστή<br>Σχετικά με το πεδίο εφαρμογής:<br>— Ελέγξτε τη διαχειριστική δήλωση και την περιγραφή των ελέγχων<br>— Ελέγξτε τη δήλωση εφαρμογής<br>Σχετικά με τη διασφάλιση:<br>— Ελέγξτε τα πορίσματα της έκθεσης<br>— Ελέγξτε τις επιστολές ενδιάμεσων διαστημάτων, εάν χρειάζεται |
| MDSCert (GSMA) (εφόσον υπάρχει) | Κινητές διατάξεις | Σχετικά με τον εκδότη:<br>— Ελέγξτε τις απαιτήσεις για τους οργανισμούς πιστοποίησης<br>Σχετικά με το πεδίο εφαρμογής:<br>— Ελέγξτε το επίπεδο διασφάλισης της ασφάλειας<br>— Ελέγξτε τις απαιτήσεις του σχήματος<br>Σχετικά με τη διασφάλιση:<br>— Ελέγξτε τις δραστηριότητες και τα πορίσματα της έκθεσης |
| Άλλα σχήματα | Οποιοδήποτε συστατικό στοιχείο | Σχετικά με το σχήμα:<br>— Ελέγξτε τη συνάφεια και τις διατάξεις του σχήματος<br>Σχετικά με τον εκδότη:<br>— Ελέγξτε τις απαιτήσεις για τους οργανισμούς πιστοποίησης<br>Σχετικά με το πεδίο εφαρμογής:<br>— Ελέγξτε τις απαιτήσεις του σχήματος<br>— Ελέγξτε τον στόχο ασφάλειας ή παρόμοιο έγγραφο που περιγράφει τις λειτουργικές απαιτήσεις και τις απαιτήσεις διασφάλισης όσον αφορά την ασφάλεια<br>— Ελέγξτε την περιγραφή του προϊόντος και επιλεγμένες λειτουργικές απαιτήσεις ασφάλειας<br>Σχετικά με τη διασφάλιση:<br>— Ελέγξτε τις δραστηριότητες και τα πορίσματα της έκθεσης |

*ΠΑΡΑΡΤΗΜΑ III*

**ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΥΛΟΠΟΙΗΣΕΙΣ ΠΟΡΤΟΦΟΛΙΟΥ**

Σύμφωνα με το άρθρο 5α παράγραφοι 4, 5, 8 και 14 του κανονισμού (ΕΕ) αριθ. 910/2014, τα λειτουργικά κριτήρια που πρέπει να πληροί μια πιστοποιημένη υλοποίηση πορτοφολιού και το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται περιλαμβάνουν τις λειτουργικές απαιτήσεις για τις πράξεις που παρατίθενται στους ακόλουθους κανονισμούς:

1) Εκτελεστικός κανονισμός (ΕΕ) 2024/2979 της Επιτροπής ([1]) για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την ακεραιότητα και τις βασικές λειτουργίες·

2) Εκτελεστικός κανονισμός (ΕΕ) 2024/2982 της Επιτροπής ([2]) για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα πρωτόκολλα και τις διεπαφές που πρέπει να υποστηρίζονται από το ευρωπαϊκό πλαίσιο για την ψηφιακή ταυτότητα·

3) Εκτελεστικός κανονισμός (ΕΕ) 2024/2977 της Επιτροπής ([3]) για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα δεδομένα ταυτοποίησης προσώπου και τις ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται για τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας.

([1]) Εκτελεστικός κανονισμός (ΕΕ) 2024/2979 της Επιτροπής, της 28ης Νοεμβρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την ακεραιότητα και τις βασικές λειτουργίες (ΕΕ L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Εκτελεστικός κανονισμός (ΕΕ) 2024/2982 της Επιτροπής, της 28ης Νοεμβρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα πρωτόκολλα και τις διεπαφές που πρέπει να υποστηρίζονται από το ευρωπαϊκό πλαίσιο για την ψηφιακή ταυτότητα (ΕΕ L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Εκτελεστικός κανονισμός (ΕΕ) 2024/2977 της Επιτροπής, της 28ης Νοεμβρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα δεδομένα ταυτοποίησης προσώπου και τις ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται για τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας (ΕΕ L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

*ΠΑΡΑΡΤΗΜΑ IV*

**ΜΕΘΟΔΟΙ ΚΑΙ ΔΙΑΔΙΚΑΣΙΕΣ ΓΙΑ ΤΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΑΞΙΟΛΟΓΗΣΗΣ**

1. **Έλεγχος της εφαρμογής υλοποίησης πορτοφολιού**

Η δραστηριότητα αξιολόγησης της συμμόρφωσης συνίσταται στην επιλογή συγκεκριμένων δραστηριοτήτων αξιολόγησης.

Τα εθνικά σχήματα πιστοποίησης προσδιορίζουν μια δραστηριότητα αξιολόγησης για την αξιολόγηση των παρεχόμενων πληροφοριών, η οποία καλύπτει τουλάχιστον τα ακόλουθα:

α) ανάλυση των παρεχόμενων πληροφοριών για να επιβεβαιωθεί ότι είναι κατάλληλες για μία από τις αρχιτεκτονικές που προσδιορίζονται στα εθνικά σχήματα πιστοποίησης·

β) ανάλυση της κάλυψης των κινδύνων και των απειλών κυβερνοασφάλειας που προσδιορίζονται στο μητρώο κινδύνων του παραρτήματος Ι από τις περιγραφόμενες διαδικασίες ασφάλειας.

Η ανάλυση που αναφέρεται στα στοιχεία α) έως β) βασίζεται στο σκεπτικό και στην αιτιολόγηση που παρέχει ο πάροχος πορτοφολιού.

2. **Δραστηριότητες αξιολόγησης που σχετίζονται με την ασφαλή κρυπτογραφική διάταξη πορτοφολιού**

1) Οι κρίσιμες λειτουργίες, συμπεριλαμβανομένων των κρυπτογραφικών υπολογισμών, δεν απαιτείται να εφαρμόζονται πλήρως στην WSCD. Ωστόσο, το μέρος που εφαρμόζεται στην WSCD, όταν λειτουργεί ως μέρος της υλοποίησης πορτοφολιού, εγγυάται την προστασία των κρίσιμων λειτουργιών που εκτελεί έναντι επιθέσεων υψηλού κινδύνου σύμφωνα με τον εκτελεστικό κανονισμό (ΕΕ) 2015/1502 της Επιτροπής ([1]).

2) Η WSCD ή μέρος αυτής μπορεί να εμπίπτει στο αντικείμενο της πιστοποίησης όταν παρέχεται από τον κάτοχο του πιστοποιητικού ή τον αιτούντα, ή να μην εμπίπτει στο αντικείμενό της όταν είναι ενσωματωμένη σε διάταξη που παρέχεται από τον τελικό χρήστη. Επιπλέον, τα εθνικά σχήματα πιστοποίησης προσδιορίζουν τις δραστηριότητες αξιολόγησης για την επαλήθευση της καταλληλότητας της WSCD, στις δύο ακόλουθες περιπτώσεις:

   α) εάν η WSCA εξαρτάται από τη συγκεκριμένη WSCD (δηλαδή εάν πρέπει να αξιολογηθεί ως σύνθετο προϊόν με βάση την WSCD), η αξιολόγηση της WSCA απαιτεί πρόσβαση σε πρόσθετες πληροφορίες σχετικά με την πιστοποίηση της WSCD, συμπεριλαμβανομένης, ιδίως, της τεχνικής έκθεσης αξιολόγησής της·

   β) εάν μια αρχιτεκτονική που εξετάζεται στο πλαίσιο του σχήματος χρησιμοποιεί περισσότερες WSCD, ή εάν ορισμένες από τις λειτουργίες σε κρίσιμα περιουσιακά στοιχεία εκτελούνται εκτός της WSCD, τότε τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν δραστηριότητες αξιολόγησης ώστε να διασφαλίζεται ότι η συνολική υλοποίηση προσφέρει το αναμενόμενο επίπεδο ασφάλειας.

3) Ως προϋπόθεση για την πιστοποίηση στο πλαίσιο των εθνικών σχημάτων πιστοποίησης, η WSCD αξιολογείται με βάση τις απαιτήσεις υψηλού επιπέδου διασφάλισης, όπως ορίζονται στον εκτελεστικό κανονισμό (ΕΕ) 2015/1502.

   Όταν πληρούνται οι προϋποθέσεις του άρθρου 3 παράγραφος 3 στοιχείο β), η αξιολόγηση της WSCD ή μέρους αυτής περιλαμβάνει αξιολόγηση τρωτότητας, όπως ορίζεται στο πρότυπο EN ISO/IEC 15408-3:2022 σε επίπεδο AVA_VAN.5, όπως ορίζεται στο παράρτημα Ι του εκτελεστικού κανονισμού (ΕΕ) 2024/482 της Επιτροπής ([2]), εκτός εάν αιτιολογείται δεόντως στον οργανισμό πιστοποίησης ότι τα χαρακτηριστικά ασφάλειας της WSCA καθιστούν δυνατή τη χρήση χαμηλότερου επιπέδου αξιολόγησης, με παράλληλη διατήρηση του ίδιου συνολικού υψηλού επιπέδου διασφάλισης με εκείνο που προβλέπεται στον εκτελεστικό κανονισμό (ΕΕ) 2015/1502.

([1]) Εκτελεστικός κανονισμός (ΕΕ) 2015/1502 της Επιτροπής, της 8ης Σεπτεμβρίου 2015, σχετικά με τη θέσπιση ελάχιστων τεχνικών προδιαγραφών και διαδικασιών για τα επίπεδα διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης σύμφωνα με το άρθρο 8 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (ΕΕ L 235 της 9.9.2015, σ. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([2]) Εκτελεστικός κανονισμός (ΕΕ) 2024/482 της Επιτροπής, 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) (ΕΕ L, 2024/482 της 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

4) Επιπλέον, στην τεκμηρίωση που σχετίζεται με κάθε συγκεκριμένη αρχιτεκτονική, τα εθνικά σχήματα πιστοποίησης διατυπώνουν παραδοχές για την εν λόγω αξιολόγηση της WSCD βάσει των οποίων μπορεί να παρέχεται αντίσταση έναντι επιθέσεων υψηλού κινδύνου σύμφωνα με τον εκτελεστικό κανονισμό (ΕΕ) 2015/1502, και προσδιορίζουν τις δραστηριότητες αξιολόγησης για την επιβεβαίωση των εν λόγω παραδοχών και προκειμένου να επιβεβαιωθεί, μετά την έκδοση του πιστοποιητικού, ότι οι παραδοχές εξακολουθούν να επαληθεύονται. Τα εθνικά σχήματα απαιτούν επίσης από τους υποψηφίους να επεξεργάζονται περαιτέρω τις εν λόγω παραδοχές για τη συγκεκριμένη εφαρμογή τους και να περιγράφουν τα μέτρα που εφαρμόζονται για να διασφαλίζεται ότι οι παραδοχές επαληθεύονται καθ' όλη τη διάρκεια του κύκλου ζωής της πιστοποίησης.

5) Σε κάθε περίπτωση, τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν δραστηριότητα αξιολόγησης για να επαληθεύεται ότι οι πληροφορίες διασφάλισης που διατίθενται για την WSCD είναι κατάλληλες για τον σκοπό της υλοποίησης πορτοφολιού, μέσω ανάλυσης των πληροφοριών διασφάλισης, όπως ο στόχος ασφάλειας για τα πιστοποιητικά EUCC, συμπεριλαμβανομένων των ακόλουθων δραστηριοτήτων:

   α) επαλήθευση ότι το αντικείμενο της αξιολόγησης είναι κατάλληλο, το οποίο για τα πιστοποιητικά EUCC, για παράδειγμα, σημαίνει επαλήθευση του ότι ο στόχος ασφάλειας είναι η συμμόρφωση με ένα από τα προφίλ προστασίας που συνιστώνται στο EUCC·

   β) επαλήθευση ότι οι παραδοχές σχετικά με το λειτουργικό περιβάλλον είναι συμβατές με την υλοποίηση πορτοφολιού, το οποίο για τα πιστοποιητικά EUCC, για παράδειγμα, σημαίνει ότι οι παραδοχές αυτές περιλαμβάνονται στον στόχο ασφάλειας·

   γ) επαλήθευση ότι οι συστάσεις που περιέχονται στις οδηγίες χρήσης ή στην τεκμηρίωση είναι συμβατές με τους όρους υπό τους οποίους πρόκειται να χρησιμοποιηθεί η WSCD στην υλοποίηση πορτοφολιού·

   δ) επαλήθευση ότι οι παραδοχές που γίνονται με βάση το εθνικό σχήμα πιστοποίησης σχετικά με τις WSCD επαληθεύονται και καλύπτονται στις πληροφορίες διασφάλισης.

6) Σε περιπτώσεις στις οποίες ορισμένες από τις επαληθεύσεις δεν είναι απολύτως πειστικές, τα εθνικά σχήματα πιστοποίησης απαιτούν από τους οργανισμούς πιστοποίησης να προσδιορίζουν απαιτήσεις αντιστάθμισης για την ασφαλή κρυπτογραφική εφαρμογή πορτοφολιού (WSCA) με βάση την WSCD, οι οποίες πρέπει να περιλαμβάνονται στην αξιολόγηση της WSCA. Εάν αυτό δεν είναι εφικτό, τα εθνικά συστήματα πιστοποίησης θεωρούν την WSCD ακατάλληλη, κάτι που σημαίνει ότι δεν εκδίδεται πιστοποιητικό συμμόρφωσης για την υλοποίηση πορτοφολιού.

3. **Δραστηριότητες αξιολόγησης που σχετίζονται με την ασφαλή κρυπτογραφική εφαρμογή πορτοφολιού (WSCA)**

1) Τα εθνικά σχήματα πιστοποίησης απαιτούν η WSCA, ως μέρος υλοποίησης πορτοφολιού, να αξιολογείται με βάση τις απαιτήσεις τουλάχιστον υψηλού επιπέδου διασφάλισης, όπως ορίζονται στον εκτελεστικό κανονισμό (ΕΕ) 2015/1502.

2) Η εν λόγω αξιολόγηση περιλαμβάνει αξιολόγηση τρωτότητας, όπως ορίζεται στο πρότυπο EN ISO/IEC 15408-3:2022 σε επίπεδο AVA_VAN.5, όπως ορίζεται στο παράρτημα Ι του εκτελεστικού κανονισμού (ΕΕ) 2024/482, εκτός εάν αιτιολογείται δεόντως στον οργανισμό πιστοποίησης ότι τα χαρακτηριστικά ασφάλειας της WSCA καθιστούν δυνατή τη χρήση χαμηλότερου επιπέδου αξιολόγησης, με παράλληλη διατήρηση του ίδιου συνολικού υψηλού επιπέδου διασφάλισης με εκείνο που προβλέπεται στον εκτελεστικό κανονισμό (ΕΕ) 2015/1502.

3) Όταν η WSCA δεν παρέχεται από τον πάροχο πορτοφολιού, τα εθνικά σχήματα πιστοποίησης διατυπώνουν παραδοχές για την εν λόγω αξιολόγηση της WSCA βάσει των οποίων μπορεί να παρέχεται αντίσταση έναντι επιθέσεων υψηλού κινδύνου σύμφωνα με τον εκτελεστικό κανονισμό (ΕΕ) 2015/1502, και προσδιορίζουν τις δραστηριότητες αξιολόγησης για την επιβεβαίωση των εν λόγω παραδοχών και προκειμένου να επιβεβαιωθεί, μετά την έκδοση του πιστοποιητικού, ότι οι παραδοχές εξακολουθούν να επαληθεύονται. Τα εθνικά σχήματα απαιτούν επίσης από τους υποψηφίους να επεξεργάζονται περαιτέρω τις εν λόγω παραδοχές για τη συγκεκριμένη εφαρμογή τους και να περιγράφουν τα μέτρα που εφαρμόζονται για να διασφαλίζεται ότι οι παραδοχές επαληθεύονται καθ' όλη τη διάρκεια του κύκλου ζωής της πιστοποίησης.

4) Σε κάθε περίπτωση, τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν δραστηριότητα αξιολόγησης για να επαληθεύεται ότι οι πληροφορίες διασφάλισης που διατίθενται για την WSCA είναι κατάλληλες για τον σκοπό της υλοποίησης πορτοφολιού, μέσω ανάλυσης των πληροφοριών διασφάλισης, όπως ο στόχος ασφάλειας για τα πιστοποιητικά EUCC, συμπεριλαμβανομένων των ακόλουθων δραστηριοτήτων:

   α) επαλήθευση ότι το αντικείμενο της αξιολόγησης είναι κατάλληλο, το οποίο για τα πιστοποιητικά EUCC, για παράδειγμα, σημαίνει επαλήθευση του ότι ο στόχος ασφάλειας είναι η συμμόρφωση με ένα από τα προφίλ προστασίας που συνιστώνται στο EUCC·

   β) επαλήθευση ότι οι παραδοχές σχετικά με το λειτουργικό περιβάλλον είναι συμβατές με την υλοποίηση πορτοφολιού, το οποίο για τα πιστοποιητικά EUCC, για παράδειγμα, σημαίνει ότι οι παραδοχές αυτές περιλαμβάνονται στον στόχο ασφάλειας·

γ) επαλήθευση ότι οι συστάσεις που περιέχονται στις οδηγίες χρήσης ή στην τεκμηρίωση είναι συμβατές με τους όρους υπό τους οποίους πρόκειται να χρησιμοποιηθεί η WSCA στην υλοποίηση πορτοφολιού·

δ) επαλήθευση ότι οι παραδοχές που γίνονται στο εθνικό σχήμα πιστοποίησης σχετικά με τις WSCA επαληθεύονται και καλύπτονται στις πληροφορίες διασφάλισης.

5) Τα εθνικά σχήματα πιστοποίησης απαιτούν η αξιολόγηση της WSCA να καλύπτει όλες τις διαδικασίες ασφάλειας τις οποίες εφαρμόζει η συγκεκριμένη WSCA.

4. **Δραστηριότητες αξιολόγησης σχετικά με τη διάταξη τελικού χρήστη**

Δεδομένου ότι το μητρώο κινδύνων, όπως ορίζεται στο παράρτημα Ι του παρόντος κανονισμού, εντοπίζει κινδύνους που συνδέονται άμεσα με την ασφάλεια της διάταξης τελικού χρήστη, τα εθνικά σχήματα πιστοποίησης καθορίζουν απαιτήσεις ασφάλειας για τις διατάξεις τελικού χρήστη. Ωστόσο, δεδομένου ότι οι εν λόγω διατάξεις παρέχονται από τον τελικό χρήστη και όχι από τον πάροχο πορτοφολιού, οι απαιτήσεις αυτές καλύπτονται από παραδοχές.

Για κάθε παραδοχή, η υλοποίηση πορτοφολιού περιλαμβάνει μηχανισμό με τον οποίο επαληθεύεται για κάθε μονάδα πορτοφολιού ότι η υποκείμενη διάταξη τελικού χρήστη πληροί την παραδοχή. Οι μηχανισμοί αυτοί θεωρούνται έλεγχοι ασφάλειας και καλύπτονται από δραστηριότητες αξιολόγησης για να αποδειχθεί τόσο η καταλληλότητά τους όσο και η αποτελεσματικότητά τους στο κατάλληλο επίπεδο διασφάλισης.

Ακολουθούν δύο παραδείγματα:

α) μια διάταξη τελικού χρήστη μπορεί να περιλαμβάνει πιστοποιημένη WSCD, η οποία πρέπει να αποδεικνύεται. Κατά κανόνα, αυτό γίνεται με τη χρήση κρυπτογραφικού μηχανισμού για την επαλήθευση της παρουσίας στην πιστοποιημένη WSCD κρυπτογραφικού απορρήτου που είναι διαθέσιμο μόνο στην πιστοποιημένη WSCD. Στην περίπτωση αυτήν, το εν λόγω κρυπτογραφικό απόρρητο θα πρέπει να θεωρείται κρίσιμο περιουσιακό στοιχείο και να καλύπτεται από την πιστοποίηση της WSCD και/ή της WSCA·

β) μια τυπική απαίτηση για τις διατάξεις τελικού χρήστη θα ήταν ότι οι διατάξεις πρέπει να λαμβάνουν ενημερώσεις ασφαλείας. Δεδομένου ότι η απαίτηση αυτή σχετίζεται με το στιγμιότυπο πορτοφολιού, ο μηχανισμός που χρησιμοποιείται για την επαλήθευση της διαθεσιμότητας ενημερώσεων ασφαλείας πρέπει να καλύπτεται μόνο από δραστηριότητες αξιολόγησης σε επίπεδο διασφάλισης κατάλληλο για το στιγμιότυπο πορτοφολιού, ιδίως επειδή είναι πιθανό να ενσωματωθεί στο στιγμιότυπο πορτοφολιού.

5. **Δραστηριότητες αξιολόγησης που σχετίζονται με το στιγμιότυπο πορτοφολιού**

1) Κατά την αξιολόγηση του στιγμιότυπου πορτοφολιού λαμβάνονται υπόψη οι ακόλουθες δύο κύριες προκλήσεις:

α) το στιγμιότυπο πορτοφολιού είναι πιθανό να υπάρχει σε ένα σύνολο παραλλαγών της ίδιας βασικής εφαρμογής, με την κάθε παραλλαγή να είναι εξειδικευμένη για συγκεκριμένη κατηγορία διατάξεων τελικού χρήστη·

β) οι διάφορες παραλλαγές του στιγμιότυπου πορτοφολιού ενδέχεται να χρειάζονται συχνές ενημερώσεις προκειμένου να ακολουθούν την ανάπτυξη της υποκείμενης πλατφόρμας ασφάλειας, για παράδειγμα όταν εντοπίζονται τρωτά σημεία που απαιτούν αλλαγές στις εφαρμογές.

2) Κατά την αξιολόγηση του στιγμιότυπου πορτοφολιού λαμβάνονται υπόψη αυτές οι ειδικές προκλήσεις. Μία από τις άμεσες συνέπειες είναι ότι το πλαίσιο των κοινών κριτηρίων ενδέχεται να μην είναι κατάλληλο σε όλες τις περιπτώσεις. Ως εκ τούτου, εξετάζονται εναλλακτικές μεθοδολογίες αξιολόγησης, όπου είναι αναγκαίο. Τα εθνικά σχήματα πιστοποίησης εξετάζουν τη χρήση της μεθοδολογίας EN 17640:2018 για τα ακόλουθα:

α) στο πλαίσιο του ίδιου του σχήματος·

β) μέσω εθνικών σχημάτων που βασίζονται στη μεθοδολογία·

γ) μέσω εθνικών σχημάτων που βασίζονται σε παρόμοιες αρχές, αλλά δημιουργήθηκαν πριν από την ανάπτυξη της μεθοδολογίας EN 17640:2018.

3) Επιπλέον, δεδομένου ότι η διενέργεια πλήρους ειδικής αξιολόγησης για κάθε παραλλαγή ενδέχεται να έχει περιορισμένη προστιθέμενη αξία, τα εθνικά σχήματα πιστοποίησης εξετάζουν το ενδεχόμενο προσδιορισμού κριτηρίων που επιτρέπουν τη διενέργεια δειγματοληψίας, προκειμένου να αποφεύγεται η επανάληψη πανομοιότυπων δραστηριοτήτων αξιολόγησης και να δίνεται έμφαση σε δραστηριότητες που αφορούν ειδικά μια συγκεκριμένη παραλλαγή. Τα εθνικά σχήματα πιστοποίησης απαιτούν από όλους τους οργανισμούς πιστοποίησης να αιτιολογούν τη χρήση δειγματοληψίας.

4) Τα εθνικά σχήματα πιστοποίησης περιλαμβάνουν επικαιροποιήσεις του στιγμιότυπου πορτοφολιού στη συνολική διαδικασία διαχείρισης αλλαγών που καθορίζεται για την υλοποίηση πορτοφολιού. Θεσπίζουν επίσης κανόνες σχετικά με τις διαδικασίες που πρέπει να εφαρμόζει ο πάροχος πορτοφολιού για κάθε επικαιροποίηση (π.χ. ανάλυση του αντικτύπου των αλλαγών στις διαδικασίες ασφάλειας), καθώς και σχετικά με τις δραστηριότητες αξιολόγησης που εκτελούνται από τον φορέα πιστοποίησης σχετικά με τις επικαιροποιήσεις υπό συγκεκριμένες συνθήκες (π.χ. αξιολόγηση της λειτουργικής αποτελεσματικότητας τροποποιημένου ελέγχου ασφάλειας). Η διαδικασία διαχείρισης αλλαγών είναι μία από τις διαδικασίες των οποίων η λειτουργική αποτελεσματικότητα πρέπει να ελέγχεται ετησίως σύμφωνα με το άρθρο 18 παράγραφος 3.

6. **Δραστηριότητες αξιολόγησης που σχετίζονται με τις υπηρεσίες και τις διαδικασίες που χρησιμοποιούνται για την παροχή και τη λειτουργία της υλοποίησης πορτοφολιού**

1) Για την αξιολόγηση των υπηρεσιών και των διαδικασιών που διαδραματίζουν ρόλο στην παροχή και τη λειτουργία της υλοποίησης πορτοφολιού και του σχήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται, η ομάδα αξιολόγησης συλλέγει αποδεικτικά στοιχεία με τη διεξαγωγή δραστηριοτήτων αξιολόγησης που μπορεί να περιλαμβάνουν δραστηριότητες ελέγχου, επιθεώρησης, επαλήθευσης και επικύρωσης.

2) Ο οργανισμός πιστοποίησης επιβεβαιώνει την επάρκεια και την καταλληλότητα των αποδεικτικών στοιχείων για την παροχή επαρκούς διασφάλισης ότι οι υπηρεσίες και οι διαδικασίες πληρούν τις απαιτήσεις πιστοποίησης, επιβεβαιώνοντας τα ακόλουθα:

   α) την ακρίβεια των πληροφοριών που παρουσιάζονται στην περιγραφή των διαδικασιών και των υπηρεσιών·

   β) την καταλληλότητα του σχεδιασμού και των ελέγχων των διαδικασιών και των υπηρεσιών για την εκπλήρωση των κριτηρίων αξιολόγησης·

   γ) τη λειτουργική αποτελεσματικότητα της εφαρμογής των εν λόγω ελέγχων κατά τη διάρκεια συγκεκριμένης περιόδου πριν από την αξιολόγηση.

3) Η ακρίβεια της περιγραφής και η λειτουργική αποτελεσματικότητα της εφαρμογής των ελέγχων μπορούν να θεωρηθούν στόχοι επαλήθευσης, κατά την έννοια του προτύπου ISO/IEC 17000:2020, των αντίστοιχων ισχυρισμών του παρόχου πορτοφολιού (δηλαδή επιβεβαίωση του δίκαιου χαρακτήρα των γεγονότων που έχουν ήδη συμβεί ή των αποτελεσμάτων που έχουν ήδη επιτευχθεί), ενώ η καταλληλότητα του σχεδιασμού και των ελέγχων των υπηρεσιών και των διαδικασιών για την εκπλήρωση των κριτηρίων αξιολόγησης μπορεί να θεωρηθεί ως στόχος επικύρωσης, κατά την έννοια του προτύπου ISO/IEC 17000: 2020, του αντίστοιχου ισχυρισμού του παρόχου πορτοφολιού (δηλαδή. επιβεβαίωση της ευλογοφάνειας όσον αφορά σκοπούμενη μελλοντική χρήση ή προβλεπόμενο αποτέλεσμα).

4) Δεδομένου ότι μια υλοποίηση πορτοφολιού δεν επιτρέπεται να λειτουργεί προτού πιστοποιηθεί, η λειτουργική αποτελεσματικότητα δεν μπορεί να επιβεβαιωθεί με βάση την πραγματική λειτουργία της υλοποίησης. Ως εκ τούτου, αυτή επιβεβαιώνεται με τη χρήση αποδεικτικών στοιχείων που συλλέγονται κατά τη διάρκεια δοκιμών ή πιλοτικής εφαρμογής.

5) Ενδέχεται να υπάρχουν ήδη εθνικά σχήματα πιστοποίησης για συγκεκριμένες υπηρεσίες και διαδικασίες, για παράδειγμα για την ένταξη των χρηστών. Η χρήση των εν λόγω σχημάτων εξετάζεται από τα εθνικά συστήματα πιστοποίησης, κατά περίπτωση.

7. **Δραστηριότητες αξιολόγησης που σχετίζονται με τις υπηρεσίες ΤΠΕ που χρησιμοποιούνται για την παροχή και τη λειτουργία της υλοποίησης πορτοφολιού**

1) Ορισμένες αρχιτεκτονικές πορτοφολιών μπορεί να βασίζονται σε ειδικές υπηρεσίες ΤΠΕ, συμπεριλαμβανομένων των υπηρεσιών υπολογιστικού νέφους για την παροχή και τη λειτουργία μιας υλοποίησης πορτοφολιού, και οι υπηρεσίες αυτές ενδέχεται να φιλοξενούν ευαίσθητα δεδομένα, καθώς και ευαίσθητες δραστηριότητες. Στην περίπτωση αυτήν, τα εθνικά σχήματα πιστοποίησης προσδιορίζουν απαιτήσεις ασφάλειας για τις εν λόγω υπηρεσίες ΤΠΕ.

2) Υπάρχουν ήδη πολλά σχήματα πιστοποίησης για υπηρεσίες ΤΠΕ, υπηρεσίες υπολογιστικού νέφους και άλλες πηγές πληροφοριών διασφάλισης, συμπεριλαμβανομένων εκείνων που παρατίθενται στο παράρτημα ΙΙ. Τα εθνικά σχήματα πιστοποίησης βασίζονται, εφόσον είναι διαθέσιμοι και κατά περίπτωση, στους εν λόγω υφιστάμενους μηχανισμούς, μέσω ενός από τους ακόλουθους μηχανισμούς:

   α) επιβολή της χρήσης συγκεκριμένου σχήματος ή επιλογής σχημάτων, με τον προσδιορισμό των όρων υπό τους οποίους οι υπηρεσίες ΤΠΕ ή υπολογιστικού νέφους πρέπει να αξιολογούνται με τη χρήση αυτών των σχημάτων·

   β) παροχή στον πάροχο πορτοφολιού της δυνατότητας να επιλέξει την αξιολόγηση και χρήση της δραστηριότητας ανάλυσης εξάρτησης για την ανάλυση της καταλληλότητας των πληροφοριών διασφάλισης που λαμβάνονται μέσω των εν λόγω αξιολογήσεων.

3) Και στις δύο περιπτώσεις, τα εθνικά σχήματα πιστοποίησης προσδιορίζουν πρόσθετες δραστηριότητες αξιολόγησης, ανάλογα με τις ανάγκες, για την ανάλυση ή τη συμπλήρωση των πληροφοριών που λαμβάνονται μέσω των εν λόγω σχημάτων.

*ΠΑΡΑΡΤΗΜΑ V*

**ΚΑΤΑΛΟΓΟΣ ΔΗΜΟΣΙΑ ΔΙΑΘΕΣΙΜΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΣΧΕΤΙΚΑ ΜΕ ΤΑ ΠΟΡΤΟΦΟΛΙΑ**

1. Οι πληροφορίες που δημοσιοποιούνται σύμφωνα με το άρθρο 8 παράγραφος 5 περιλαμβάνουν τουλάχιστον τα ακόλουθα:

   α) τυχόν περιορισμούς στη χρήση μιας υλοποίησης πορτοφολιού·

   β) καθοδήγηση και συστάσεις από τον πάροχο πορτοφολιού για την παροχή βοήθειας στους τελικούς χρήστες όσον αφορά την ασφαλή διαμόρφωση, εγκατάσταση, εφαρμογή, λειτουργία και συντήρηση πορτοφολιών·

   γ) την περίοδο κατά την οποία θα προσφέρεται υποστήριξη ασφαλείας προς τους τελικούς χρήστες, ιδίως όσον αφορά τη διαθεσιμότητα επικαιροποιήσεων σχετικών με την κυβερνοασφάλεια·

   δ) τα στοιχεία επικοινωνίας του κατασκευαστή ή του παρόχου και τις αποδεκτές μεθόδους για τη λήψη πληροφοριών από τελικούς χρήστες και ερευνητές ασφαλείας σχετικά με τρωτά σημεία·

   ε) αναφορά σε επιγραμμικά αποθετήρια που περιλαμβάνουν δημοσιοποιημένα τρωτά σημεία που σχετίζονται με πορτοφόλια και σε τυχόν σχετικές συμβουλές για την κυβερνοασφάλεια.

2. Οι πληροφορίες που αναφέρονται στην παράγραφο 1 διατίθενται με σαφή, περιεκτικό και εύκολα προσβάσιμο τρόπο, σε δημόσια προσβάσιμο χώρο, σε κάθε πρόσωπο που επιθυμεί να χρησιμοποιήσει υλοποίηση πορτοφολιού.

*ΠΑΡΑΡΤΗΜΑ VI*

**ΜΕΘΟΔΟΛΟΓΙΑ ΓΙΑ ΤΗΝ ΑΞΙΟΛΟΓΗΣΗ ΤΗΣ ΑΠΟΔΟΧΗΣ ΠΛΗΡΟΦΟΡΙΩΝ ΔΙΑΣΦΑΛΙΣΗΣ**

1. **Αξιολόγηση της διαθεσιμότητας τεκμηρίωσης διασφάλισης**

Οι αξιολογητές παραθέτουν την τεκμηρίωση διασφάλισης που είναι διαθέσιμη για κάθε σχετικό συστατικό στοιχείο της υλοποίησης πορτοφολιού και του σχήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται. Στη συνέχεια, οι αξιολογητές αξιολογούν τη συνολική συνάφεια κάθε τεκμηρίωσης διασφάλισης για την εξέταση της εξάρτησης.

Κατά την ανάλυση λαμβάνονται υπόψη οι ακόλουθες πτυχές:

1) σχετικά με την ίδια την τεκμηρίωση διασφάλισης:

   α) το είδος της τεκμηρίωσης διασφάλισης, με όλες τις απαιτούμενες λεπτομέρειες

   (παραδείγματα τέτοιων εγγράφων είναι τα πιστοποιητικά συμμόρφωσης σύμφωνα με το πρότυπο EN ISO/IEC 27001:2022 ή τύπου 1 ή τύπου 2 για εκθέσεις ISAE)·

   β) η καλυπτόμενη περίοδος ή η διάρκεια ισχύος

   [η περίοδος αυτή μπορεί να συμπληρωθεί με επιστολή ενδιάμεσου διαστήματος (έγγραφο που καλύπτει χρονικό διάστημα μεταξύ της ημερομηνίας λήξης της περιόδου αναφοράς της τρέχουσας έκθεσης ISAE και της δημοσίευσης νέας έκθεσης ISAE) ή παρόμοια δήλωση]·

   γ) το εφαρμοστέο πλαίσιο (π.χ. υφιστάμενο πρότυπο)·

   δ) αν η τεκμηρίωση διασφάλισης περιλαμβάνει χαρτογράφηση των απαιτήσεων του σχήματος·

2) σχετικά με την επαγγελματική επάρκεια και αμεροληψία του εκδότη της έκθεσης διασφάλισης:

   α) ονομασία του οργανισμού πιστοποίησης και, εάν υπάρχει, ονοματεπώνυμο του επικεφαλής αξιολογητή·

   β) αποδεικτικά στοιχεία της ικανότητας του οργανισμού πιστοποίησης και του αξιολογητή (π.χ. διαπίστευση, προσωπική πιστοποίηση κ.λπ.)·

   γ) αποδεικτικά στοιχεία της αμεροληψίας του οργανισμού πιστοποίησης και του αξιολογητή (π.χ. διαπίστευση κ.λπ.).

2. **Αξιολόγηση της αξιοπιστίας σχετικά με τις επιμέρους απαιτήσεις**

Οι αξιολογητές επαληθεύουν ότι η τεκμηρίωση διασφάλισης που διατίθεται για την υλοποίηση πορτοφολιού και το σχήμα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται επαρκεί για να διαπιστωθεί ότι η υλοποίηση πορτοφολιού ανταποκρίνεται στις προσδοκίες σε σχέση με τις επιμέρους απαιτήσεις του σχήματος πιστοποίησης.

Η εν λόγω αξιολόγηση διενεργείται για κάθε σχετικό συστατικό στοιχείο της υλοποίησης πορτοφολιού και του σχήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται, με τη διατύπωση παραδοχής σχετικά με τους ελέγχους ασφάλειας της υλοποίησης πορτοφολιού.

Για κάθε τέτοια παραδοχή, η ομάδα αξιολόγησης καθορίζει αν η βεβαιότητα που παρέχεται στη διαθέσιμη τεκμηρίωση διασφάλισης είναι επαρκής ή όχι.

Η διαπίστωση ότι η διασφάλιση είναι επαρκής βασίζεται στα ακόλουθα:

1) οι απαιτούμενες πληροφορίες είναι διαθέσιμες, με το αναμενόμενο επίπεδο βεβαιότητας, στην τεκμηρίωση διασφάλισης·

2) οι πληροφορίες που διατίθενται στην τεκμηρίωση διασφάλισης δεν καλύπτουν το πλήρες πεδίο εφαρμογής της απαίτησης, αλλά πρόσθετοι έλεγχοι ή αντισταθμιστικοί έλεγχοι (δηλαδή εσωτερικοί έλεγχοι που μειώνουν τον κίνδυνο υφιστάμενης ή δυνητικής αδυναμίας ελέγχου) που εφαρμόζονται στην υλοποίηση πορτοφολιού ή στο σχήμα ηλεκτρονικής ταυτοποίησης βάσει του οποίου αυτή παρέχεται επιτρέπουν στους αξιολογητές να διαπιστώσουν ότι οι πληροφορίες είναι επαρκείς·

3) οι πληροφορίες που είναι διαθέσιμες στην τεκμηρίωση διασφάλισης δεν προσφέρουν το αναμενόμενο επίπεδο διασφάλισης, αλλά οι έλεγχοι που εφαρμόζονται για την αξιολόγηση και την παρακολούθηση του παρόχου πορτοφολιού επιτρέπουν στους αξιολογητές να διαπιστώσουν ότι οι πληροφορίες είναι επαρκείς·

4) εάν στην τεκμηρίωση διασφάλισης αναφέρονται περιπτώσεις μη συμμόρφωσης όσον αφορά τον σχεδιασμό ή την εφαρμογή των ελέγχων που χρησιμοποιούνται για την εκπλήρωση μιας παραδοχής, τα διορθωτικά μέτρα που προτείνονται και εφαρμόζονται από τον πάροχο πορτοφολιού και εξετάζονται από τους αξιολογητές του είναι επαρκή ώστε να διασφαλίζεται ότι πράγματι πληρούται η παραδοχή.

*ΠΑΡΑΡΤΗΜΑ VII*

**ΠΕΡΙΕΧΟΜΕΝΟ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΥΜΜΟΡΦΩΣΗΣ**

1. Μοναδικό αναγνωριστικό που χορηγείται από τον οργανισμό πιστοποίησης που εκδίδει το πιστοποιητικό συμμόρφωσης.

2. Πληροφορίες σχετικά με την πιστοποιημένη υλοποίηση πορτοφολιού και τα συστήματα ηλεκτρονικής ταυτοποίησης βάσει των οποίων αυτή παρέχεται, καθώς και σχετικά με τον κάτοχο του πιστοποιητικού συμμόρφωσης, συμπεριλαμβανομένων των ακόλουθων:

   α) ονομασία της υλοποίησης πορτοφολιού·

   β) ονομασία των συστημάτων ηλεκτρονικής ταυτοποίησης βάσει των οποίων παρέχεται η υλοποίηση πορτοφολιού·

   γ) έκδοση της υλοποίησης πορτοφολιού που αξιολογήθηκε·

   δ) όνομα, διεύθυνση και στοιχεία επικοινωνίας του κατόχου του πιστοποιητικού συμμόρφωσης·

   ε) σύνδεσμος προς τον ιστότοπο του κατόχου του πιστοποιητικού συμμόρφωσης που περιέχει τις πληροφορίες που απαιτείται να δημοσιοποιούνται.

3. Πληροφορίες σχετικά με την αξιολόγηση και την πιστοποίηση της υλοποίησης πορτοφολιού και των συστημάτων ηλεκτρονικής ταυτοποίησης στο πλαίσιο των οποίων αυτή παρέχεται, συμπεριλαμβανομένων των ακόλουθων:

   α) όνομα, διεύθυνση και στοιχεία επικοινωνίας του οργανισμού πιστοποίησης που εξέδωσε το πιστοποιητικό συμμόρφωσης·

   β) εάν είναι διαφορετικός από τον οργανισμό πιστοποίησης, όνομα του οργανισμού αξιολόγησης της συμμόρφωσης που διενήργησε την αξιολόγηση, μαζί με πληροφορίες σχετικά με τη διαπίστευσή του·

   γ) όνομα του ιδιοκτήτη του σχήματος·

   δ) αναφορές στον κανονισμό (ΕΕ) αριθ. 910/2014 και στον παρόντα κανονισμό·

   ε) αναφορά στην έκθεση πιστοποίησης που συνδέεται με το πιστοποιητικό συμμόρφωσης·

   στ) αναφορά στην έκθεση αξιολόγησης της πιστοποίησης που συνδέεται με το πιστοποιητικό συμμόρφωσης·

   ζ) αναφορά στα πρότυπα που χρησιμοποιήθηκαν για την αξιολόγηση, συμπεριλαμβανομένων των εκδόσεών τους·

   η) ημερομηνία έκδοσης του πιστοποιητικού συμμόρφωσης·

   θ) περίοδος ισχύος του πιστοποιητικού συμμόρφωσης.

*ΠΑΡΑΡΤΗΜΑ VIII*

**ΠΕΡΙΕΧΟΜΕΝΟ ΤΗΣ ΔΗΜΟΣΙΑΣ ΕΚΘΕΣΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΚΑΙ ΤΗΣ ΕΚΘΕΣΗΣ ΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ**

1. Η δημόσια έκθεση πιστοποίησης περιέχει τουλάχιστον τις ακόλουθες πτυχές:

   α) συνοπτική παρουσίαση·

   β) προσδιορισμό της υλοποίησης πορτοφολιού και του σχήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται·

   γ) περιγραφή της υλοποίησης πορτοφολιού και του σχήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου αυτή παρέχεται·

   δ) τις πληροφορίες ασφαλείας που πρέπει να δημοσιοποιούνται, όπως περιγράφονται στο παράρτημα V, ή μνεία των εν λόγω πληροφοριών·

   ε) σύνοψη του προκαταρκτικού σχεδίου ελέγχου και επικύρωσης·

   στ) περίληψη της εξέτασης και της απόφασης πιστοποίησης.

2. Η έκθεση αξιολόγησης της πιστοποίησης περιλαμβάνει τουλάχιστον τα εξής:

   α) περιγραφή του σχεδιασμού της υλοποίησης πορτοφολιού, του συστήματος ταυτοποίησης και της διαδικασίας ένταξης, μαζί με την εκτίμηση κινδύνου και το συγκεκριμένο σχέδιο επικύρωσης·

   β) περιγραφή του τρόπου με τον οποίο η υλοποίηση πορτοφολιού πληροί τις απαιτήσεις υψηλού επιπέδου διασφάλισης και του τρόπου με τον οποίο αυτό αποδεικνύεται από τα αποτελέσματα της αξιολόγησης της υλοποίησης πορτοφολιού που διενεργήθηκε σύμφωνα με τον παρόντα κανονισμό·

   γ) περιγραφή του αποτελέσματος της αξιολόγησης της συμμόρφωσης της υλοποίησης πορτοφολιού και του σχήματος ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχονται οι αντίστοιχες μονάδες πορτοφολιού, ιδίως της συμμόρφωσης με τα ακόλουθα:

      — τις απαιτήσεις του άρθρου 5α παράγραφοι 4, 5 και 8 του κανονισμού (ΕΕ) αριθ. 910/2014·

      — τις απαιτήσεις λογικού διαχωρισμού που καθορίζονται στο άρθρο 5α παράγραφος 14 του κανονισμού (ΕΕ) αριθ. 910/2014, και

      — κατά περίπτωση, τα πρότυπα και τις τεχνικές προδιαγραφές που αναφέρονται στο άρθρο 5α παράγραφος 24 του κανονισμού (ΕΕ) αριθ. 910/2014, με παράλληλη περιγραφή του τρόπου με τον οποίο οι εν λόγω απαιτήσεις σχετίζονται με τις αντίστοιχες κανονιστικές απαιτήσεις που καθορίζονται από τα εθνικά σχήματα πιστοποίησης·

   δ) σύνοψη του αποτελέσματος της εκτέλεσης του σχεδίου επικύρωσης, συμπεριλαμβανομένων όλων των περιπτώσεων μη συμμόρφωσης που εντοπίστηκαν.

*ΠΑΡΑΡΤΗΜΑ IX*

**ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ ΓΙΑ ΤΙΣ ΥΠΟΧΡΕΩΤΙΚΕΣ ΑΞΙΟΛΟΓΗΣΕΙΣ ΕΠΟΠΤΕΙΑΣ**

1. Το άρθρο 18 καθορίζει απαιτήσεις για τον κύκλο ζωής της πιστοποίησης, ιδίως για την εκτέλεση τακτικών δραστηριοτήτων αξιολόγησης. Οι εν λόγω δραστηριότητες περιλαμβάνουν τουλάχιστον τα ακόλουθα:

   α) πλήρη αξιολόγηση του αντικειμένου της εκτίμησης της συμμόρφωσης στην αρχική αξιολόγηση και σε κάθε αξιολόγηση επαναπιστοποίησης, συμπεριλαμβανομένου ενός χαρακτηριστικού επικαιροποίησης οποιουδήποτε συστατικού στοιχείου του προϊόντος·

   β) εκτίμηση τρωτότητας στην αρχική αξιολόγηση και σε κάθε αξιολόγηση επαναπιστοποίησης, και τουλάχιστον ανά διετία σε αξιολογήσεις εποπτείας, η οποία καλύπτει τουλάχιστον τις αλλαγές στο αντικείμενο της εκτίμησης της συμμόρφωσης και τις αλλαγές στο περιβάλλον απειλών μετά την τελευταία εκτίμηση τρωτότητας·

   γ) πρόσθετες δραστηριότητες, όπως δοκιμές διείσδυσης σε περίπτωση αυξημένου επιπέδου κινδύνου ή εμφάνισης νέων απειλών·

   δ) αξιολόγηση της λειτουργικής αποτελεσματικότητας των διαδικασιών συντήρησης τουλάχιστον κάθε χρόνο στις αξιολογήσεις εποπτείας και επαναπιστοποίησης, η οποία καλύπτει τουλάχιστον τις διαδικασίες ελέγχου έκδοσης, ενημερώσεων και διαχείρισης τρωτών σημείων·

   ε) κατόπιν επιτυχούς εξέτασης και έκδοσης απόφασης πιστοποίησης, την έκδοση πιστοποιητικού συμμόρφωσης μετά την αρχική αξιολόγηση και μετά από κάθε αξιολόγηση επαναπιστοποίησης.

2. Στον πίνακα 1 παρατίθεται χρονοδιάγραμμα αναφοράς βάσει 4ετούς κύκλου, όπου:

   α) το έτος 1 αρχίζει με την πρώτη έκδοση του πιστοποιητικού συμμόρφωσης· και

   β) όλες οι δραστηριότητες αξιολόγησης εκτελούνται εντός 12 μηνών από την αξιολόγηση του προηγούμενου έτους.

3. Το χρονοδιάγραμμα που παρατίθεται στον πίνακα 1 αποτελεί σύσταση για τη διασφάλιση της έγκαιρης επαναπιστοποίησης και την αποφυγή διαταραχών στην παροχή της υλοποίησης πορτοφολιού. Και άλλα χρονοδιαγράμματα είναι δυνατά, εφόσον η ισχύς του πιστοποιητικού συμμόρφωσης δεν υπερβαίνει τα πέντε έτη, όπως ορίζεται στο άρθρο 5γ παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 910/2014.

4. Εκτός από τις τακτικές αξιολογήσεις, μπορεί να διενεργηθεί ειδική αξιολόγηση κατόπιν αιτήματος του οργανισμού πιστοποίησης ή του κατόχου του πιστοποιητικού συμμόρφωσης, μετά από σημαντική αλλαγή στο αντικείμενο της πιστοποίησης ή στο περιβάλλον απειλών.

5. Οποιαδήποτε αξιολόγηση, συμπεριλαμβανομένων των αξιολογήσεων εποπτείας και των ειδικών αξιολογήσεων, μπορεί να οδηγήσει στην έκδοση νέου πιστοποιητικού συμμόρφωσης, ιδίως σε περίπτωση σημαντικών αλλαγών στο αντικείμενο της πιστοποίησης, αλλά με την ίδια ημερομηνία λήξης με το αρχικό πιστοποιητικό συμμόρφωσης.

*Πίνακας 1*

**Πλήρης 4ετής κύκλος αξιολόγησης**

| Ώρα | Τύπος αξιολ. | Δραστηριότητες |
|---|---|---|
| Έτος 0 | Αρχική | — Πλήρης αξιολόγηση του αντικειμένου της πιστοποίησης, συμπεριλαμβανομένης εκτίμησης τρωτότητας<br>— Συμπερίληψη ενός χαρακτηριστικού για την εκτέλεση ενημερώσεων σε κάθε στοιχείο του λογισμικού<br>— Αξιολόγηση των διαδικασιών συντήρησης, εξαιρουμένης της λειτουργικής αποτελεσματικότητάς τους<br>— Έκδοση του πιστοποιητικού συμμόρφωσης και έναρξη του 4ετούς κύκλου |
| Έτος 1 | Εποπτεία | — Αξιολόγηση της λειτουργικής αποτελεσματικότητας των διαδικασιών συντήρησης<br>— Τουλάχιστον έλεγχος έκδοσης, ενημέρωση, διαχείριση τρωτών σημείων<br>— Αξιολόγηση των αλλαγών που επηρεάζουν την ασφάλεια του προϊόντος |

| Ώρα | Τύπος αξιολ. | Δραστηριότητες |
|---|---|---|
| Έτος 2 | Εποπτεία | — Αξιολόγηση τρωτότητας της πλήρους υλοποίησης<br>— Αξιολόγηση της λειτουργικής αποτελεσματικότητας των διαδικασιών συντήρησης<br>— Τουλάχιστον έλεγχος έκδοσης, ενημέρωση, διαχείριση τρωτών σημείων<br>— Αξιολόγηση των αλλαγών που επηρεάζουν την ασφάλεια του προϊόντος |
| Έτος 3 | Εποπτεία | — Αξιολόγηση της λειτουργικής αποτελεσματικότητας των διαδικασιών συντήρησης<br>— Τουλάχιστον έλεγχος έκδοσης, ενημέρωση, διαχείριση τρωτών σημείων<br>— Αξιολόγηση των αλλαγών που επηρεάζουν την ασφάλεια του προϊόντος |
| Έτος 4 | Επαναπιστοποίηση | (1) Πλήρης αξιολόγηση του αντικειμένου της πιστοποίησης, συμπεριλαμβανομένης εκτίμησης τρωτότητας<br>(2) Απλουστευμένη αξιολόγηση για χαρακτηριστικά/διαδικασίες που δεν έχουν αλλάξει<br>(3) Συμπερίληψη ενός χαρακτηριστικού για την εκτέλεση ενημερώσεων σε κάθε στοιχείο του λογισμικού<br>(4) Αξιολόγηση των διαδικασιών συντήρησης, συμπεριλαμβανομένης της λειτουργικής αποτελεσματικότητάς τους<br>(5) Έκδοση νέου πιστοποιητικού συμμόρφωσης |