ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2015/1502 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

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

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

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 8 παράγραφος 3,

Εκτιμώντας τα ακόλουθα:

(1) Το άρθρο 8 του κανονισμού (ΕΕ) αριθ. 910/2014 προβλέπει ότι ένα σχέδιο ηλεκτρονικής ταυτοποίησης που κοινοποιείται σύμφωνα με το άρθρο 9 παράγραφος 1 πρέπει να προσδιορίζει τα επίπεδα διασφάλισης — χαμηλό, βασικό και υψηλό — των μέσων ηλεκτρονικής ταυτοποίησης που εκδίδονται στο πλαίσιο του εν λόγω σχεδίου.

(2) Ο καθορισμός των ελάχιστων τεχνικών προδιαγραφών, των προτύπων και των διαδικασιών είναι απαραίτητος προκειμένου να διασφαλιστεί η κοινή κατανόηση των λεπτομερειών σχετικά με τα επίπεδα διασφάλισης και τη διαλειτουργικότητα κατά τη χαρτογράφηση των εθνικών επιπέδων διασφάλισης των κοινοποιημένων σχεδίων ηλεκτρονικής ταυτοποίησης με βάση τα επίπεδα διασφάλισης που προβλέπονται στο άρθρο 8, όπως προβλέπει το άρθρο 12 παράγραφος 4 στοιχείο β) του κανονισμού (ΕΕ) αριθ. 910/2014.

(3) Για τις προδιαγραφές και τις διαδικασίες που καθορίζονται στην παρούσα εκτελεστική πράξη ως βασικό διεθνές πρότυπο στον τομέα των επιπέδων διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης έχει ληφθεί υπόψη το διεθνές πρότυπο ISO/IEC 29115. Ωστόσο, το περιεχόμενο του κανονισμού (ΕΕ) αριθ. 910/2014 διαφέρει από το εν λόγω διεθνές πρότυπο, ιδίως σε σχέση με τις απαιτήσεις εξακρίβωσης και επαλήθευσης ταυτότητας, καθώς και σχετικά με τον τρόπο με τον οποίο λαμβάνονται υπόψη οι διαφορές μεταξύ των διευθετήσεων των κρατών μελών όσον αφορά τις ταυτότητες και των υφιστάμενων εργαλείων της ΕΕ για τον ίδιο σκοπό. Ως εκ τούτου, το παράρτημα, αν και βασίζεται στο εν λόγω διεθνές πρότυπο, δεν πρέπει να παραπέμπει σε οποιοδήποτε συγκεκριμένο περιεχόμενο του προτύπου ISO/IEC 29115.

(4) Ο παρών κανονισμός έχει συνταχθεί ως η πλέον κατάλληλη προσέγγιση η οποία αντανακλάται επίσης στους ορισμούς που χρησιμοποιούνται για τον προσδιορισμό των όρων και εννοιών. Λαμβάνουν υπόψη το στόχο του κανονισμού (ΕΕ) αριθ. 910/2014 όσον αφορά τα επίπεδα διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης. Συνεπώς, η πιλοτική εφαρμογή μεγάλης κλίμακας STORK, συμπεριλαμβανομένων των προδιαγραφών που έχουν καταρτιστεί από αυτήν, καθώς και οι ορισμοί και οι έννοιες του ISO/IEC 29115 θα πρέπει να λαμβάνονται ιδιαιτέρως υπόψη κατά τη θέσπιση των προδιαγραφών και διαδικασιών που καθορίζονται στην παρούσα εκτελεστική πράξη.

(5) Ανάλογα με το πλαίσιο εντός του οποίου πρέπει να επαληθευτεί μια πτυχή των αποδεικτικών στοιχείων της ταυτότητας, οι έγκυρες πηγές μπορούν να λάβουν πολλές μορφές, όπως μεταξύ άλλων μητρώα, έγγραφα, φορείς. Οι έγκυρες πηγές μπορεί να διαφέρουν στα διάφορα κράτη μέλη, ακόμη και σε παρόμοιο πλαίσιο.

(6) Οι απαιτήσεις για την εξακρίβωση και την επαλήθευση της ταυτότητας θα πρέπει να λαμβάνουν υπόψη τα διάφορα συστήματα και πρακτικές, εξασφαλίζοντας παράλληλα επαρκώς υψηλή βεβαιότητα προκειμένου να διασφαλίζεται η απαραίτητη εμπιστοσύνη. Επομένως, η αποδοχή διαδικασιών που χρησιμοποιούνταν προηγουμένως για σκοπό διαφορετικό από την έκδοση μέσου ηλεκτρονικής ταυτοποίησης θα πρέπει να εξαρτάται από την επιβεβαίωση ότι οι εν λόγω διαδικασίες πληρούν τις απαιτήσεις που προβλέπονται για το αντίστοιχο επίπεδο διασφάλισης.

([1]) ΕΕ L 257 της 28.8.2014, σ. 73.

(7) Χρησιμοποιούνται συνήθως μέσα επαλήθευσης, όπως κοινά μυστικά (shared secrets), συσκευές και φυσικά χαρακτηριστικά γνωρίσματα. Ωστόσο, θα πρέπει να ενθαρρύνεται η χρήση περισσότερων μέσων επαλήθευσης, ιδίως μέσων από διαφορετικές κατηγορίες, ώστε να ενισχυθεί η ασφάλεια της διαδικασίας επαλήθευσης.

(8) Ο παρών κανονισμός δεν θα πρέπει να θίγει τα δικαιώματα εκπροσώπησης των νομικών προσώπων. Ωστόσο, το παράρτημα θα πρέπει να προβλέπει απαιτήσεις για τη σύνδεση μεταξύ των μέσων ηλεκτρονικής ταυτοποίησης φυσικών και νομικών προσώπων.

(9) Θα πρέπει να αναγνωριστεί η σημασία της ασφάλειας των πληροφοριών και των συστημάτων διαχείρισης των υπηρεσιών, όπως θα πρέπει να αναγνωριστεί και η σημασία της χρήσης αναγνωρισμένων μεθόδων και της εφαρμογής των αρχών που περιλαμβάνονται σε πρότυπα όπως τα πρότυπα των σειρών ISO/IEC 27000 και ISO/IEC 20000.

(10) Θα πρέπει επίσης να λαμβάνονται υπόψη ορθές πρακτικές στα κράτη μέλη σε σχέση με τα επίπεδα διασφάλισης.

(11) Η πιστοποίηση της ασφάλειας πληροφοριακών συστημάτων με βάση διεθνή πρότυπα αποτελεί σημαντικό εργαλείο για την εξακρίβωση της συμμόρφωσης των προϊόντων με τις προδιαγραφές της παρούσας εκτελεστικής πράξης όσον αφορά την ασφάλεια.

(12) Η επιτροπή που αναφέρεται στο άρθρο 48 του κανονισμού (ΕΚ) αριθ. 910/2014 δεν εξέδωσε γνώμη εντός της προθεσμίας που όρισε ο/η πρόεδρός της,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

1. Τα επίπεδα διασφάλισης — χαμηλό, βασικό και υψηλό — των μέσων ηλεκτρονικής ταυτοποίησης που εκδίδονται στο πλαίσιο ενός κοινοποιημένου σχεδίου ηλεκτρονικής ταυτοποίησης καθορίζονται με βάση τις προδιαγραφές και τις διαδικασίες που καθορίζονται στο παράρτημα.

2. Οι προδιαγραφές και οι διαδικασίες που καθορίζονται στο παράρτημα χρησιμοποιούνται για να προσδιοριστεί το επίπεδο διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης που εκδίδονται βάσει ενός κοινοποιημένου σχεδίου ηλεκτρονικής ταυτοποίησης με τον καθορισμό της αξιοπιστίας και της ποιότητας των ακόλουθων στοιχείων:

α) καταχώρηση, κατά τα οριζόμενα στο τμήμα 2.1 του παραρτήματος του παρόντος κανονισμού σύμφωνα με το άρθρο 8 παράγραφος 3 στοιχείο α) του κανονισμού (ΕΕ) αριθ. 910/2014·

β) διαχείριση μέσων ηλεκτρονικής ταυτοποίησης, κατά τα οριζόμενα στο τμήμα 2.2 του παραρτήματος του παρόντος κανονισμού σύμφωνα με το άρθρο 8 παράγραφος 3 στοιχεία β) και στ) του κανονισμού (ΕΕ) αριθ. 910/2014·

γ) επαλήθευση ταυτότητας, κατά τα οριζόμενα στο τμήμα 2.3 του παραρτήματος του παρόντος κανονισμού σύμφωνα με το άρθρο 8 παράγραφος 3 στοιχείο γ) του κανονισμού (ΕΕ) αριθ. 910/2014·

δ) διαχείριση και οργάνωση, κατά τα οριζόμενα στο τμήμα 2.4 του παραρτήματος του παρόντος κανονισμού σύμφωνα με το άρθρο 8 παράγραφος 3 στοιχεία δ) και ε) του κανονισμού (ΕΕ) αριθ. 910/2014.

3. Όταν τα μέσα ηλεκτρονικής ταυτοποίησης που εκδίδονται βάσει ενός κοινοποιημένου σχεδίου ηλεκτρονικής ταυτοποίησης πληρούν μια απαίτηση που περιλαμβάνεται σε υψηλότερο επίπεδο διασφάλισης, τεκμαίρεται ότι πληρούν την αντίστοιχη απαίτηση χαμηλότερου επιπέδου διασφάλισης.

4. Εκτός εάν ορίζεται διαφορετικά στο σχετικό μέρος του παραρτήματος, προκειμένου να καλυφθεί το σκοπούμενο επίπεδο διασφάλισης, πληρούνται όλα τα στοιχεία που απαριθμούνται στο παράρτημα, για συγκεκριμένο επίπεδο διασφάλισης του μέσου ηλεκτρονικής ταυτοποίησης που έχει εκδοθεί βάσει ενός κοινοποιημένου σχεδίου ηλεκτρονικής ταυτοποίησης.

Άρθρο 2

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 8 Σεπτεμβρίου 2015.

Για την Επιτροπή

Ο Πρόεδρος

Jean-Claude JUNCKER

ΠΑΡΑΡΤΗΜΑ

Τεχνικές προδιαγραφές και διαδικασίες για τα επίπεδα διασφάλισης — χαμηλό, βασικό και υψηλό — των μέσων ηλεκτρονικής ταυτοποίησης που εκδίδονται βάσει κοινοποιημένου σχεδίου ηλεκτρονικής ταυτοποίησης

1. **Ισχύοντες ορισμοί**

Για τους σκοπούς του παρόντος παραρτήματος, εφαρμόζονται οι ακόλουθοι ορισμοί:

1) «έγκυρη πηγή»: οιαδήποτε πηγή, ανεξάρτητα από τη μορφή της, η οποία μπορεί να χρησιμοποιηθεί για την παροχή επακριβών δεδομένων, πληροφοριών και/ή αποδεικτικών στοιχείων που να μπορούν να χρησιμοποιηθούν προς απόδειξη ταυτότητας·

2) «μέσο επαλήθευσης ταυτότητας»: μέσο το οποίο έχει επιβεβαιωθεί ότι συνδέεται με ένα πρόσωπο και το οποίο εμπίπτει σε μια από τις ακόλουθες κατηγορίες:

α) «μέσο επαλήθευσης ταυτότητας με βάση την κατοχή»: μέσο επαλήθευσης ταυτότητας για το οποίο το άτομο απαιτείται να αποδείξει ότι το μέσο βρίσκεται στην κατοχή του·

β) «μέσο επαλήθευσης ταυτότητας με βάση τη γνώση»: μέσο επαλήθευσης ταυτότητας για το οποίο το άτομο απαιτείται να αποδείξει ότι έχει γνώση του εν λόγω μέσου·

γ) «μέσο εγγενούς επαλήθευσης ταυτότητας»: μέσο επαλήθευσης ταυτότητας που βασίζεται σε ένα σωματικό χαρακτηριστικό ενός φυσικού προσώπου, και για το οποίο το άτομο απαιτείται να αποδείξει ότι διαθέτει το συγκεκριμένο σωματικό χαρακτηριστικό·

3) «δυναμική επαλήθευση ταυτότητας»: ηλεκτρονική διαδικασία η οποία χρησιμοποιεί κρυπτογράφηση ή άλλες τεχνικές για να εξασφαλίσει ένα μέσο δημιουργίας, κατόπιν αιτήματος, ηλεκτρονικής απόδειξης ότι ότι το άτομο έχει τον έλεγχο ή κατέχει τα στοιχεία ταυτότητας και η οποία αλλάζει για κάθε επαλήθευση ταυτότητας μεταξύ του ατόμου και του συστήματος επαλήθευσης της ταυτότητας του ατόμου·

4) «σύστημα διαχείρισης της ασφάλειας των πληροφοριών»: σύνολο διεργασιών και διαδικασιών για τη διαχείριση σε αποδεκτό επίπεδο, των κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριών.

2. **Τεχνικές προδιαγραφές και διαδικασίες**

Τα στοιχεία των τεχνικών προδιαγραφών και των διαδικασιών που περιγράφονται στο παρόν παράρτημα χρησιμοποιούνται για τον προσδιορισμό του τρόπου με τον οποίο οι απαιτήσεις και τα κριτήρια του άρθρου 8 του κανονισμού (ΕΕ) αριθ. 910/2014 εφαρμόζονται για τα μέσα ηλεκτρονικής ταυτοποίησης που εκδίδονται βάσει σχεδίου ηλεκτρονικής ταυτοποίησης.

2.1. *Καταχώριση:*

2.1.1. Αίτηση και καταχώριση

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Διασφάλιση ότι ο αιτών είναι ενήμερος για τους όρους και τις προϋποθέσεις που συνδέονται με τη χρήση των μέσων ηλεκτρονικής ταυτοποίησης. 2. Διασφάλιση ότι ο αιτών είναι ενήμερος για τις προτεινόμενες προφυλάξεις ασφαλείας που συνδέονται με τα μέσα ηλεκτρονικής ταυτοποίησης. 3. Συλλογή των σχετικών στοιχείων ταυτότητας που απαιτούνται για την απόδειξη και την επαλήθευση της ταυτότητας.
Βασικό	Ταυτίζεται με το χαμηλό επίπεδο.
Υψηλό	Ταυτίζεται με το χαμηλό επίπεδο.

2.1.2. Απόδειξη και επαλήθευση της ταυτότητας (φυσικό πρόσωπο)

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Το άτομο μπορεί να θεωρηθεί ότι κατέχει αποδεικτικά στοιχεία τα οποία αναγνωρίζονται από το κράτος μέλος στο οποίο υποβάλλεται η αίτηση για το μέσο ηλεκτρονικής ταυτοποίησης, και τα οποία αντιπροσωπεύουν τη δηλωθείσα ταυτότητα. 2. Τα αποδεικτικά στοιχεία μπορούν να θεωρηθούν πραγματικά, ή ότι υφίστανται σύμφωνα με έγκυρη πηγή και τα αποδεικτικά στοιχεία φαίνεται ότι είναι έγκυρα. 3. Είναι γνωστό από έγκυρη πηγή ότι η δηλωθείσα ταυτότητα υφίσταται και μπορεί να θεωρηθεί ότι το πρόσωπο που διεκδικεί την ταυτότητα είναι ένα και το αυτό.
Βασικό	Χαμηλό επίπεδο, και πρέπει να πληρούται μία από τις εναλλακτικές επιλογές που αναφέρονται στα σημεία 1 έως 4: 1. Έχει επαληθευτεί ότι το άτομο κατέχει αποδεικτικά στοιχεία τα οποία αναγνωρίζονται από το κράτος μέλος στο οποίο υποβάλλεται η αίτηση για το μέσο ηλεκτρονικής ταυτοποίησης, και τα οποία αντιπροσωπεύουν τη δηλωθείσα ταυτότητα και τα αποδεικτικά στοιχεία ελέγχονται, προκειμένου να διαπιστωθεί ότι είναι γνήσια· ή, σύμφωνα με μια έγκυρη πηγή, είναι γνωστό ότι υπάρχουν και σχετίζονται με κάποιο πραγματικό πρόσωπο και έχουν ληφθεί μέτρα για την ελαχιστοποίηση του κινδύνου η ταυτότητα του προσώπου να μην είναι η δηλωθείσα ταυτότητα, λαμβάνοντας υπόψη, για παράδειγμα, τον κίνδυνο απώλειας, κλοπής, αναστολής, ανάκλησης ή λήξης της ισχύος των αποδεικτικών στοιχείων. Ή 2. Υποβάλλεται έγγραφο ταυτότητας κατά τη διάρκεια της διαδικασίας καταχώρισης στο κράτος μέλος όπου έχει εκδοθεί το έγγραφο και το έγγραφο φαίνεται ότι σχετίζεται με το πρόσωπο που το προσκομίζει και έχουν ληφθεί μέτρα για την ελαχιστοποίηση του κινδύνου η ταυτότητα του προσώπου να μην είναι η δηλωθείσα ταυτότητα, λαμβάνοντας υπόψη, για παράδειγμα, τον κίνδυνο απώλειας, κλοπής, αναστολής, ανάκλησης ή λήξης της ισχύος των εγγράφων. Ή 3. Όταν οι διαδικασίες που έχουν χρησιμοποιηθεί προηγουμένως από δημόσιο ή ιδιωτικό φορέα στο ίδιο κράτος μέλος για άλλο σκοπό από την έκδοση μέσου ηλεκτρονικής ταυτοποίησης, παρέχουν ισοδύναμη διασφάλιση με εκείνες που ορίζονται στο σημείο 2.1.2 για το βασικό επίπεδο διασφάλισης, τότε η οντότητα που ευθύνεται για την καταχώριση, δεν χρειάζεται να επαναλάβει τις προηγούμενες διαδικασίες, υπό τον όρο ότι η εν λόγω ισοδύναμη διασφάλιση επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του κανονισμού (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [1], ή από ισοδύναμο φορέα. Ή 4. Όταν εκδίδονται μέσα ηλεκτρονικής ταυτοποίησης βάσει έγκυρων κοινοποιημένων μέσων ηλεκτρονικής ταυτοποίησης με βασικό ή υψηλό επίπεδο διασφάλισης, και λαμβανομένων υπόψη των κινδύνων μεταβολής των στοιχείων ταυτοποίησης προσώπου, δεν απαιτείται να επαναληφθούν οι διαδικασίες εξακρίβωσης και επαλήθευσης της ταυτότητας. Όταν το μέσο ηλεκτρονικής ταυτοποίησης που χρησιμεύει ως βάση δεν έχει κοινοποιηθεί, το βασικό ή υψηλό επίπεδο διασφάλισης πρέπει να επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του κανονισμού (ΕΚ) αριθ. 765/2008 ή από ισοδύναμο φορέα.

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Υψηλό	Πρέπει να πληρούνται οι απαιτήσεις των σημείων 1 και 2: 1. Βασικό επίπεδο, και πρέπει να πληρούται μία από τις εναλλακτικές επιλογές που αναφέρονται στα σημεία α έως γ: α) Όταν το πρόσωπο έχει επαληθευθεί ότι διαθέτει φωτογραφία ή βιομετρικά στοιχεία ταυτοποίησης που αναγνωρίζονται από το κράτος μέλος στο οποίο υποβλήθηκε η αίτηση για το μέσο ηλεκτρονικής ταυτότητας, και τα εν λόγω αποδεικτικά στοιχεία αντιπροσωπεύουν τη δηλωθείσα ταυτότητα, τα αποδεικτικά στοιχεία ελέγχονται προκειμένου να διαπιστωθεί ότι είναι έγκυρα σύμφωνα με έγκυρη πηγή· και ο αιτών ταυτοποιείται με τη δηλωθείσα ταυτότητα με σύγκριση ενός ή περισσότερων σωματικών χαρακτηριστικών του προσώπου με έγκυρη πηγή· ή β) Όταν οι διαδικασίες που έχουν χρησιμοποιηθεί προηγουμένως από δημόσιο ή ιδιωτικό φορέα στο ίδιο κράτος μέλος για άλλο σκοπό από την έκδοση μέσου ηλεκτρονικής ταυτοποίησης, παρέχουν ισοδύναμη διασφάλιση με εκείνες που ορίζονται στο σημείο 2.1.2 για το υψηλό επίπεδο διασφάλισης, τότε η οντότητα που ευθύνεται για την καταχώριση, δεν χρειάζεται να επαναλάβει τις προηγούμενες διαδικασίες, υπό τον όρο ότι η εν λόγω ισοδύναμη διασφάλιση επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του κανονισμού (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, ή από ισοδύναμο φορέα και λαμβάνονται μέτρα για να αποδειχτεί ότι τα αποτελέσματα των προηγούμενων διαδικασιών εξακολουθούν να ισχύουν· ή γ) Όταν εκδίδονται μέσα ηλεκτρονικής ταυτοποίησης βάσει έγκυρων κοινοποιημένων μέσων ηλεκτρονικής ταυτοποίησης με βασικό ή υψηλό επίπεδο διασφάλισης, και λαμβανομένων υπόψη των κινδύνων μεταβολής των στοιχείων ταυτοποίησης προσώπου, δεν απαιτείται να επαναληφθούν οι διαδικασίες εξακρίβωσης και επαλήθευσης της ταυτότητας. Όταν το μέσο ηλεκτρονικής ταυτοποίησης που χρησιμεύει ως βάση δεν έχει κοινοποιηθεί, το υψηλό επίπεδο διασφάλισης πρέπει να επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του κανονισμού (ΕΚ) αριθ. 765/2008 ή από ισοδύναμο φορέα. και λαμβάνονται μέτρα για να αποδειχθεί ότι τα αποτελέσματα της εν λόγω προηγούμενης διαδικασίας έκδοσης του κοινοποιημένου μέσου ηλεκτρονικής ταυτοποίησης εξακολουθούν να ισχύουν. Ή 2. Εάν ο αιτών δεν υποβάλει κάποια αναγνωρισμένη φωτογραφία ή βιομετρικά στοιχεία ταυτοποίησης, εφαρμόζονται οι ίδιες διαδικασίες που εφαρμόζονται σε εθνικό επίπεδο στο κράτος μέλος του φορέα που είναι αρμόδιος για την καταχώρηση όσον αφορά την απόκτηση αναγνωρισμένης φωτογραφίας ή των βιομετρικών στοιχείων ταυτοποίησης.

([1]) 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).

2.1.3. Απόδειξη και επαλήθευση της ταυτότητας (νομικό πρόσωπο)

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Η δηλωθείσα ταυτότητα του νομικού προσώπου αποδεικνύεται με βάση αποδεικτικά στοιχεία τα οποία αναγνωρίζονται από το κράτος μέλος στο οποίο υποβάλλεται η αίτηση για το μέσο ηλεκτρονικής ταυτότητας.

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
	2. Τα αποδεικτικά στοιχεία φαίνεται να είναι έγκυρα και μπορεί να υποτεθεί ότι είναι γνήσια ή ότι υφίστανται σύμφωνα με έγκυρη πηγή, εφόσον η καταχώριση του νομικού προσώπου στην έγκυρη πηγή είναι προαιρετική και διέπεται από διευθέτηση μεταξύ του νομικού προσώπου και της έγκυρης πηγής. 3. Δεν είναι σε γνώση της έγκυρης πηγής ότι το νομικό πρόσωπο είναι σε κατάσταση που να το εμποδίζει να ενεργεί ως το εν λόγω νομικό πρόσωπο.
Βασικό	Χαμηλό επίπεδο, και πρέπει να πληρούται μία από τις εναλλακτικές επιλογές που αναφέρονται στα σημεία 1 έως 3: 1. Η δηλωθείσα ταυτότητα του νομικού προσώπου αποδεικνύεται με βάση αποδεικτικά στοιχεία τα οποία αναγνωρίζονται από το κράτος μέλος στο οποίο υποβάλλεται η αίτηση για το μέσο ηλεκτρονικής ταυτότητας, συμπεριλαμβανομένων του ονόματος, της νομικής μορφής και (εάν απαιτείται) του αριθμού μητρώου του νομικού προσώπου· και τα αποδεικτικά στοιχεία ελέγχονται, προκειμένου να εκτιμηθεί κατά πόσον είναι γνήσια, ή είναι γνωστό ότι υπάρχουν σύμφωνα με μια έγκυρη πηγή, εφόσον η εγγραφή του νομικού προσώπου στην έγκυρη πηγή απαιτείται ώστε το νομικό πρόσωπο να μπορεί να λειτουργήσει εντός του οικείου κλάδου· και έχουν ληφθεί μέτρα για την ελαχιστοποίηση του κινδύνου η ταυτότητα του νομικού προσώπου να μην είναι η δηλωθείσα ταυτότητα, λαμβάνοντας υπόψη, για παράδειγμα, τον κίνδυνο απώλειας, κλοπής, αναστολής, ανάκλησης ή λήξης της ισχύος των εγγράφων. Ή 2. Όταν οι διαδικασίες που έχουν χρησιμοποιηθεί προηγουμένως από δημόσιο ή ιδιωτικό φορέα στο ίδιο κράτος μέλος για άλλο σκοπό από την έκδοση μέσου ηλεκτρονικής ταυτοποίησης, παρέχουν ισοδύναμη διασφάλιση με εκείνες που ορίζονται στο σημείο 2.1.3 για το βασικό επίπεδο διασφάλισης, τότε η οντότητα που ευθύνεται για την καταχώριση, δεν χρειάζεται να επαναλάβει τις προηγούμενες διαδικασίες, υπό τον όρο ότι η εν λόγω ισοδύναμη διασφάλιση επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του κανονισμού (ΕΚ) αριθ. 765/2008, ή από ισοδύναμο φορέα. Ή 3. Όταν εκδίδονται μέσα ηλεκτρονικής ταυτοποίησης βάσει έγκυρων κοινοποιημένων μέσων ηλεκτρονικής ταυτοποίησης με βασικό ή υψηλό επίπεδο διασφάλισης, δεν απαιτείται να επαναληφθούν οι διαδικασίες εξακρίβωσης και επαλήθευσης της ταυτότητας. Όταν το μέσο ηλεκτρονικής ταυτοποίησης που χρησιμεύει ως βάση δεν έχει κοινοποιηθεί, το βασικό ή υψηλό επίπεδο διασφάλισης ς πρέπει να επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του κανονισμού (ΕΚ) αριθ. 765/2008 ή από ισοδύναμο φορέα.
Υψηλό	Βασικό επίπεδο, και πρέπει να πληρούται μία από τις εναλλακτικές επιλογές που αναφέρονται στα σημεία 1 έως 3: 1. Η δηλωθείσα ταυτότητα του νομικού προσώπου αποδεικνύεται με βάση αποδεικτικά στοιχεία τα οποία αναγνωρίζονται από το κράτος μέλος στο οποίο υποβάλλεται η αίτηση για το μέσο ηλεκτρονικής ταυτότητας, συμπεριλαμβανομένων του ονόματος, της νομικής μορφής και τουλάχιστον ενός μοναδικού χαρακτηριστικού που εκπροσωπεί το νομικό πρόσωπο σε εθνικό πλαίσιο· και τα αποδεικτικά στοιχεία ελέγχονται, προκειμένου να διαπιστωθεί ότι είναι γνήσια σύμφωνα με έγκυρη πηγή. Ή

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
	2. Όταν οι διαδικασίες που έχουν χρησιμοποιηθεί προηγουμένως από δημόσιο ή ιδιωτικό φορέα στο ίδιο κράτος μέλος για άλλο σκοπό από την έκδοση μέσου ηλεκτρονικής ταυτοποίησης, παρέχουν ισοδύναμη διασφάλιση με εκείνες που ορίζονται στο σημείο 2.1.3 για το υψηλό επίπεδο διασφάλισης, τότε η οντότητα που ευθύνεται για την καταχώριση, δεν χρειάζεται να επαναλάβει τις προηγούμενες διαδικασίες, υπό τον όρο ότι η εν λόγω ισοδύναμη διασφάλιση επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του κανονισμού (ΕΚ) αριθ. 765/2008, ή από ισοδύναμο φορέα· και λαμβάνονται μέτρα για να αποδειχτεί ότι τα αποτελέσματα της εν λόγω προηγούμενης διαδικασίας εξακολουθούν να ισχύουν. Ή 3. Όταν εκδίδονται μέσα ηλεκτρονικής ταυτοποίησης βάσει έγκυρων κοινοποιημένων μέσων ηλεκτρονικής ταυτοποίησης με υψηλό επίπεδο διασφάλισης, δεν απαιτείται να επαναληφθούν οι διαδικασίες εξακρίβωσης και επαλήθευσης της ταυτότητας. Όταν το μέσο ηλεκτρονικής ταυτοποίησης που χρησιμεύει ως βάση δεν έχει κοινοποιηθεί, το υψηλό επίπεδο διασφάλισης πρέπει να επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης που αναφέρεται στο άρθρο 2 παράγραφος 13 του κανονισμού (ΕΚ) αριθ. 765/2008 ή από ισοδύναμο φορέα· και λαμβάνονται μέτρα για να αποδειχθεί ότι τα αποτελέσματα της εν λόγω προηγούμενης διαδικασίας έκδοσης του κοινοποιημένου μέσου ηλεκτρονικής ταυτοποίησης εξακολουθούν να ισχύουν.

2.1.4. Σύνδεση μεταξύ των μέσων ηλεκτρονικής ταυτοποίησης φυσικών και νομικών προσώπων

Κατά περίπτωση, για τη σύνδεση μεταξύ του μέσου ηλεκτρονικής ταυτοποίησης ενός φυσικού προσώπου και του μέσου ηλεκτρονικής ταυτοποίησης ενός νομικού προσώπου («σύνδεση»), πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις:

1) Είναι δυνατή η αναστολή και/ή η ανάκληση της σύνδεσης. Η διαχείριση του κύκλου ζωής μιας σύνδεσης (π.χ. ενεργοποίηση, αναστολή, ανανέωση, ανάκληση) πραγματοποιείται σύμφωνα με διαδικασίες αναγνωρισμένες σε εθνικό επίπεδο.

2) Το φυσικό πρόσωπο του οποίου το μέσο ηλεκτρονικής ταυτοποίησης συνδέεται με το μέσο ηλεκτρονικής ταυτοποίησης του νομικού προσώπου μπορεί να εξουσιοδοτήσει, σύμφωνα με διαδικασίες αναγνωρισμένες σε εθνικό επίπεδο, άλλο φυσικό πρόσωπο να ασκήσει τη σύνδεση. Ωστόσο, το φυσικό πρόσωπο που εξουσιοδοτεί παραμένει υπεύθυνο.

3) Η σύνδεση πραγματοποιείται με τον ακόλουθο τρόπο:

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Η εξακρίβωση της ταυτότητας του φυσικού προσώπου που ενεργεί για λογαριασμό του νομικού προσώπου επαληθεύεται ως πραγματοποιηθείσα σε χαμηλό επίπεδο ή ανώτερο. 2. Η σύνδεση έχει καθοριστεί σύμφωνα με διαδικασίες αναγνωρισμένες σε εθνικό επίπεδο. 3. Δεν είναι σε γνώση της έγκυρης πηγής ότι το φυσικό πρόσωπο είναι σε κατάσταση που να το εμποδίζει να ενεργεί ως το νομικό πρόσωπο.
Βασικό	Σημείο 3 χαμηλού επιπέδου, συν: 1. Η εξακρίβωση της ταυτότητας του φυσικού προσώπου που ενεργεί για λογαριασμό του νομικού προσώπου επαληθεύεται ως πραγματοποιηθείσα σε βασικό ή υψηλό επίπεδο.

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
	2. Η σύνδεση καθορίζεται σύμφωνα με διαδικασίες αναγνωρισμένες σε εθνικό επίπεδο, οι οποίες καταλήγουν στην καταχώριση της σύνδεσης σε έγκυρη πηγή. 3. Η σύνδεση έχει ελεγχθεί με βάση πληροφορίες από έγκυρη πηγή.
Υψηλό	Σημείο 3 χαμηλού επιπέδου και σημείο 2 βασικού επιπέδου, συν: 1. Η εξακρίβωση της ταυτότητας του φυσικού προσώπου που ενεργεί για λογαριασμό του νομικού προσώπου επαληθεύεται ως πραγματοποιηθείσα σε υψηλό επίπεδο. 2. Η σύνδεση έχει επαληθευτεί βάσει ενός μοναδικού χαρακτηριστικού που εκπροσωπεί το νομικό πρόσωπο σε εθνικό πλαίσιο· και με βάση τις πληροφορίες από έγκυρη πηγή που αντιπροσωπεύουν κατά τρόπο μοναδικό το φυσικό πρόσωπο.

2.2. *Διαχείριση μέσων ηλεκτρονικής ταυτοποίησης*

2.2.1. Χαρακτηριστικά και σχεδιασμός μέσων ηλεκτρονικής ταυτοποίησης

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Το μέσο ηλεκτρονικής ταυτοποίησης χρησιμοποιεί τουλάχιστον ένα μέσο επαλήθευσης της ταυτότητας. 2. Το μέσο ηλεκτρονικής ταυτοποίησης σχεδιάζεται έτσι ώστε ο εκδότης να λαμβάνει εύλογα μέτρα για να ελέγχει ότι χρησιμοποιείται μόνον υπό τον έλεγχο ή την κατοχή του προσώπου στο οποίο ανήκει.
Βασικό	1. Το μέσο ηλεκτρονικής ταυτοποίησης χρησιμοποιεί τουλάχιστον δύο μέσα επαλήθευσης της ταυτότητας διαφορετικών κατηγοριών. 2. Το μέσο ηλεκτρονικής ταυτοποίησης σχεδιάζεται έτσι ώστε να θεωρείται ότι χρησιμοποιείται μόνον υπό τον έλεγχο ή την κατοχή του προσώπου στο οποίο ανήκει.
Υψηλό	Βασικό επίπεδο, συν: 1. Το μέσο ηλεκτρονικής ταυτοποίησης προστατεύει έναντι αντιγραφής και παραποίησης καθώς και έναντι επιθέσεων υψηλού κινδύνου 2. Το μέσο ηλεκτρονικής ταυτοποίησης είναι σχεδιασμένο κατά τρόπον ώστε ο ιδιοκτήτης να μπορεί να το προστατεύσει κατά τρόπο αξιόπιστο έναντι της χρήσης του από τρίτους.

2.2.2. Έκδοση, παράδοση και ενεργοποίηση

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	Μετά την έκδοση, το μέσο ηλεκτρονικής ταυτοποίησης παραδίδεται μέσω μηχανισμού με τον οποίο εξασφαλίζεται η παράδοσή του μόνο στο προβλεπόμενο πρόσωπο.
Βασικό	Μετά την έκδοση, το μέσο ηλεκτρονικής ταυτοποίησης παραδίδεται μέσω μηχανισμού με τον οποίο εξασφαλίζεται η παράδοσή του μόνο στο πρόσωπο στο οποίο ανήκει.
Υψηλό	Η διαδικασία ενεργοποίησης επαληθεύει ότι το μέσο ηλεκτρονικής ταυτοποίησης παραδόθηκε μόνο στο πρόσωπο στο οποίο ανήκει.

2.2.3. Αναστολή, ανάκληση και επανενεργοποίηση

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Είναι δυνατόν να ανασταλεί και/ή να ανακληθεί ένα μέσο ηλεκτρονικής ταυτοποίησης με έγκαιρο και αποτελεσματικό τρόπο. 2. Ύπαρξη μέτρων που λαμβάνονται για την πρόληψη μη εξουσιοδοτημένης αναστολής, ανάκλησης και/ή επανενεργοποίησης. 3. Επανενεργοποίηση πραγματοποιείται μόνο αν συνεχίζουν να πληρούνται οι ίδιες απαιτήσεις διασφάλισης που είχαν καθοριστεί πριν από την αναστολή ή την ανάκληση.
Βασικό	Ταυτίζεται με το χαμηλό επίπεδο.
Υψηλό	Ταυτίζεται με το χαμηλό επίπεδο.

2.2.4. Ανανέωση και αντικατάσταση

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	Λαμβανομένων υπόψη των κινδύνων μεταβολής των στοιχείων ταυτοποίησης προσώπου, η ανανέωση ή η αντικατάσταση πρέπει να πληροί τις ίδιες απαιτήσεις διασφάλισης όπως η αρχική εξακρίβωση και επαλήθευση της ταυτότητας ή να βασίζεται σε έγκυρο μέσο ηλεκτρονικής ταυτοποίησης του ίδιου, ή υψηλότερου, επιπέδου διασφάλισης.
Βασικό	Ταυτίζεται με το χαμηλό επίπεδο.
Υψηλό	Χαμηλό επίπεδο, συν: Όταν η ανανέωση ή η αντικατάσταση βασίζεται σε έγκυρο μέσο ηλεκτρονικής ταυτοποίησης, τα δεδομένα ταυτότητας επαληθεύονται από έγκυρη πηγή.

2.3. *Επαλήθευση ταυτότητας*

Το παρόν τμήμα εστιάζει στους κινδύνους που συνδέονται με τη χρήση του μηχανισμού επαλήθευσης της ταυτότητας και απαριθμεί τις απαιτήσεις για κάθε επίπεδο διασφάλισης. Στο παρόν τμήμα οι έλεγχοι νοούνται ότι είναι ανάλογοι των κινδύνων στο συγκεκριμένο επίπεδο.

2.3.1. Μηχανισμός επαλήθευσης ταυτότητας

Στον ακόλουθο πίνακα καθορίζονται οι απαιτήσεις ανά επίπεδο διασφάλισης όσον αφορά τον μηχανισμό επαλήθευσης της ταυτότητας, μέσω του οποίου το φυσικό ή νομικό πρόσωπο χρησιμοποιεί το μέσο ηλεκτρονικής ταυτοποίησης για να επιβεβαιώσει την ταυτότητά του έναντι βασιζόμενου μέρους,

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Πριν από την ανακοίνωση των στοιχείων ταυτοποίησης προσώπου προηγείται αξιόπιστη επαλήθευση του μέσου ηλεκτρονικής ταυτοποίησης και της ισχύος του. 2. Όταν τα στοιχεία ταυτοποίησης προσώπου αποθηκεύονται ως μέρος του μηχανισμού επαλήθευσης της ταυτότητας, οι εν λόγω πληροφορίες διασφαλίζονται προκειμένου να προστατευθούν έναντι απώλειας και παραβίασης, συμπεριλαμβανομένης της ανάλυσης εκτός διαδικτύου. 3. Ο μηχανισμός επαλήθευσης της ταυτότητας εφαρμόζει διαδικασίες ελέγχου της ασφάλειας για την επαλήθευση του μέσου ηλεκτρονικής ταυτοποίησης, έτσι ώστε να καταστεί εξαιρετικά απίθανη η υπονόμευση των μηχανισμών επαλήθευσης ταυτότητας από εικασίες, υποκλοπές, αναπαραγωγή ή παραποίηση επικοινωνίας από επιθέσεις ενισχυμένου-βασικού κινδύνου.

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Βασικό	Χαμηλό επίπεδο, συν: 1. Πριν από την ανακοίνωση των στοιχείων ταυτοποίησης προσώπου προηγείται αξιόπιστη επαλήθευση του μέσου ηλεκτρονικής ταυτοποίησης και της ισχύος του μέσω δυναμικής επαλήθευσης της ταυτότητας. 2. Ο μηχανισμός επαλήθευσης της ταυτότητας εφαρμόζει διαδικασίες ελέγχου της ασφάλειας για την επαλήθευση του μέσου ηλεκτρονικής ταυτοποίησης, έτσι ώστε να καταστεί εξαιρετικά απίθανη η υπονόμευση των μηχανισμών επαλήθευσης ταυτότητας από εικασίες, υποκλοπές, αναπαραγωγή ή παραποίηση επικοινωνίας από επιθέσεις μεσαίου κινδύνου.
Υψηλό	Βασικό επίπεδο, συν: Ο μηχανισμός επαλήθευσης της ταυτότητας εφαρμόζει διαδικασίες ελέγχου της ασφάλειας για την επαλήθευση του μέσου ηλεκτρονικής ταυτοποίησης, έτσι ώστε να καταστεί εξαιρετικά απίθανη η υπονόμευση των μηχανισμών επαλήθευσης ταυτότητας από εικασίες, υποκλοπές, αναπαραγωγή ή παραποίηση επικοινωνίας από επιθέσεις υψηλού κινδύνου.

2.4. *Διαχείριση και οργάνωση*

Όλοι οι συμμετέχοντες που παρέχουν υπηρεσίες οι οποίες σχετίζονται με την ηλεκτρονική ταυτοποίηση σε διασυνοριακό πλαίσιο («πάροχοι») διαθέτουν τεκμηριωμένες πρακτικές διαχείρισης της ασφάλειας των πληροφοριών, πολιτικές, προσεγγίσεις της διαχείρισης των κινδύνων, και άλλες αναγνωρισμένους ελέγχους ώστε να διασφαλίζουν έναντι των αρμόδιων οργάνων διακυβέρνησης των σχεδίων ηλεκτρονικής ταυτοποίησης στα αντίστοιχα κράτη μέλη ότι εφαρμόζονται αποτελεσματικές πρακτικές. Σε όλο το σημείο 2.4, όλες οι απαιτήσεις/στοιχεία νοούνται ως ανάλογα προς τους κινδύνους στο συγκεκριμένο επίπεδο.

2.4.1. Γενικές διατάξεις

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Οι πάροχοι κάθε επιχειρησιακής υπηρεσίας που καλύπτεται από τον παρόντα κανονισμό είναι δημόσιες αρχές ή νομικές οντότητες αναγνωρισμένες από το εθνικό δίκαιο κράτους μέλους, με αναγνωρισμένη και πλήρως λειτουργική οργάνωση όσον αφορά όλα τα μέρη που σχετίζονται με την παροχή των υπηρεσιών. 2. Οι πάροχοι πληρούν τις νομικές απαιτήσεις που υπέχουν σε σχέση με τη λειτουργία και την παροχή της υπηρεσίας, συμπεριλαμβανομένου του είδους των πληροφοριών που ενδέχεται να ζητηθούν, τον τρόπο εξακρίβωσης της ταυτότητας, το είδος των πληροφοριών που ενδέχεται να διατηρηθούν και για ποιο χρονικό διάστημα. 3. Οι πάροχοι είναι σε θέση να αποδείξουν την ικανότητά τους να αναλαμβάνουν την αστική ευθύνη για ζημίες, καθώς και το ότι διαθέτουν επαρκείς οικονομικούς πόρους για τη συνέχιση της λειτουργίας και την παροχή των υπηρεσιών. 4. Οι πάροχοι είναι υπεύθυνοι για την εκπλήρωση κάθε δέσμευσης που έχει ανατεθεί σε άλλη οντότητα μέσω εξωπορισμού, και τη συμμόρφωση με την πολιτική του σχεδίου, ως εάν οι πάροχοι να είχαν εκτελέσει οι ίδιοι τα σχετικά καθήκοντα. 5. Τα σχέδια ηλεκτρονικής ταυτοποίησης που δεν έχουν θεσπιστεί με εθνική νομοθεσία διαθέτουν αποτελεσματικό σχέδιο τερματισμού. Το εν λόγω σχέδιο περιλαμβάνει ομαλή διακοπή της υπηρεσίας ή συνέχιση από άλλον πάροχο, τον τρόπο με τον οποίο θα ενημερωθούν οι αρμόδιες αρχές και οι τελικοί χρήστες, καθώς και λεπτομέρειες σχετικά με τον τρόπο προστασίας, διατήρησης και καταστροφής των αρχείων, σύμφωνα με την πολιτική του σχεδίου.
Βασικό	Ταυτίζεται με το χαμηλό επίπεδο.
Υψηλό	Ταυτίζεται με το χαμηλό επίπεδο.

2.4.2. Δημοσιευμένες ανακοινώσεις και πληροφορίες για τους χρήστες

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Ύπαρξη δημοσιευμένου ορισμού της υπηρεσίας που περιλαμβάνει όλους τους ισχύοντες όρους και προϋποθέσεις, καθώς και τα τέλη, συμπεριλαμβανομένων των ενδεχόμενων περιορισμών της χρήσης. Ο ορισμός της υπηρεσίας περιλαμβάνει και πολιτική προστασίας της ιδιωτικής ζωής. 2. Πρέπει να θεσπιστούν κατάλληλες πολιτικές και διαδικασίες ώστε να εξασφαλιστεί ότι οι χρήστες της υπηρεσίας ενημερώνονται κατά τρόπο έγκαιρο και αξιόπιστο για τυχόν αλλαγές στον ορισμό της υπηρεσίας, στους ισχύοντες όρους και προϋποθέσεις, καθώς και στην πολιτική προστασίας της ιδιωτικής ζωής της συγκεκριμένης υπηρεσίας. 3. Πρέπει να θεσπιστούν κατάλληλες πολιτικές και διαδικασίες ώστε να εξασφαλιστεί η παροχή πλήρων και ορθών απαντήσεων στα αιτήματα παροχής πληροφοριών.
Βασικό	Ταυτίζεται με το χαμηλό επίπεδο.
Υψηλό	Ταυτίζεται με το χαμηλό επίπεδο.

2.4.3. Διαχείριση της ασφάλειας των πληροφοριών

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	Υφίσταται αποτελεσματικό σύστημα διαχείρισης της ασφάλειας των πληροφοριών για τη διαχείριση και τον έλεγχο των κινδύνων για την ασφάλεια των πληροφοριών.
Βασικό	Χαμηλό επίπεδο, συν: Το σύστημα διαχείρισης της ασφάλειας των πληροφοριών εφαρμόζει δοκιμασμένα πρότυπα ή αρχές για τη διαχείριση και τον έλεγχο των κινδύνων για την ασφάλεια των πληροφοριών.
Υψηλό	Ταυτίζεται με το βασικό επίπεδο.

2.4.4. Τήρηση αρχείων

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Καταγραφή και διατήρηση συναφών πληροφοριών με χρήση αποτελεσματικού συστήματος διαχείρισης αρχείων, λαμβάνοντας υπόψη την ισχύουσα νομοθεσία και τις ορθές πρακτικές όσον αφορά την προστασία των δεδομένων και τη διατήρηση των δεδομένων. 2. Διατήρηση, στο μέτρο που επιτρέπεται από το εθνικό δίκαιο ή άλλη εθνική διοικητική ρύθμιση, και προστασία αρχείων για όσο χρόνο απαιτείται για τους σκοπούς του ελέγχου και της διερεύνησης των παραβιάσεων ασφάλειας και διατήρηση, μετά την οποία τα αρχεία πρέπει να καταστρέφονται με ασφάλεια.
Βασικό	Ταυτίζεται με το χαμηλό επίπεδο.
Υψηλό	Ταυτίζεται με το χαμηλό επίπεδο.

2.4.5. Εγκαταστάσεις και προσωπικό

Ο πίνακας που ακολουθεί περιλαμβάνει τις απαιτήσεις όσον αφορά τις εγκαταστάσεις, το προσωπικό και, κατά περίπτωση, υπεργολάβους που εκτελούν καθήκοντα τα οποία καλύπτονται από τον παρόντα κανονισμό. Η συμμόρφωση με όλες τις απαιτήσεις πρέπει να είναι ανάλογη προς τους κινδύνους που σχετίζονται με το προβλεπόμενο επίπεδο διασφάλισης.

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Ύπαρξη διαδικασιών που διασφαλίζουν ότι το προσωπικό και οι υπεργολάβοι είναι επαρκώς εκπαιδευμένοι, ειδικευμένοι και έμπειροι στις δεξιότητες που απαιτούνται για την εκτέλεση των ρόλων τους οποίους αναλαμβάνουν. 2. Ύπαρξη επαρκούς προσωπικού και υπεργολάβων για την επαρκή λειτουργία και υποστήριξη της υπηρεσίας σύμφωνα με τις οικείες πολιτικές και διαδικασίες. 3. Οι εγκαταστάσεις που χρησιμοποιούνται για την παροχή της υπηρεσίας, παρακολουθούνται και προστατεύονται συνεχώς έναντι ζημιών που προκαλούνται από περιβαλλοντικά συμβάντα, μη εξουσιοδοτημένη πρόσβαση και άλλους παράγοντες που ενδέχεται να επηρεάζουν την ασφάλεια της υπηρεσίας. 4. Στις εγκαταστάσεις που χρησιμοποιούνται για την παροχή της υπηρεσίας εξασφαλίζεται ότι η πρόσβαση σε περιοχές διατήρησης ή επεξεργασίας προσωπικών, κρυπτογραφικών ή άλλων ευαίσθητων πληροφοριών περιορίζεται στο εξουσιοδοτημένο προσωπικό ή υπεργολάβους.
Βασικό	Ταυτίζεται με το χαμηλό επίπεδο.
Υψηλό	Ταυτίζεται με το χαμηλό επίπεδο.

2.4.6. Τεχνικοί έλεγχοι

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	1. Η ύπαρξη αναλογικών τεχνικών ελέγχων για τη διαχείριση των κινδύνων στην ασφάλεια των υπηρεσιών, την προστασία του εμπιστευτικού χαρακτήρα, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που υποβάλλονται σε επεξεργασία. 2. Οι δίαυλοι ηλεκτρονικής επικοινωνίας που χρησιμοποιούνται για την ανταλλαγή προσωπικών ή ευαίσθητων πληροφοριών προστατεύονται από υποκλοπές, παραποίηση και αναπαραγωγή. 3. Η πρόσβαση σε ευαίσθητο κρυπτογραφικό υλικό, εάν αυτό χρησιμοποιείται για την έκδοση μέσου ηλεκτρονικής ταυτοποίησης και επαλήθευσης της ταυτότητας, περιορίζεται αυστηρά στους ρόλους και τις εφαρμογές που απαιτούν πρόσβαση. Εξασφαλίζεται ότι το εν λόγω υλικό δεν αποθηκεύεται ποτέ συνεχώς υπό μορφή απλού κειμένου. 4. Υφίστανται διαδικασίες ώστε να διασφαλίζεται διαχρονικά η ασφάλεια και η ικανότητα ανταπόκρισης στις αλλαγές των επιπέδων κινδύνου, στα συμβάντα και στις παραβιάσεις ασφαλείας. 5. Όλα τα μέσα που περιλαμβάνουν προσωπικές, κρυπτογραφικές ή άλλες ευαίσθητες πληροφορίες αποθηκεύονται, μεταφέρονται και απορρίπτονται κατά ασφαλή τρόπο.
Βασικό	Χαμηλό επίπεδο συν: Το ευαίσθητο κρυπτογραφικό υλικό, εάν αυτό χρησιμοποιείται για την έκδοση μέσου ηλεκτρονικής ταυτοποίησης και επαλήθευσης της ταυτότητας προστατεύεται από παρεμβάσεις παραποίησης
Υψηλό	Ταυτίζεται με το βασικό επίπεδο.

2.4.7. Συμμόρφωση και έλεγχος

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	Ύπαρξη περιοδικών εσωτερικών ελέγχων με πεδίο εφαρμογής το οποίο καλύπτει όλα τα μέρη που σχετίζονται με τις παρεχόμενες υπηρεσίες ώστε να εξασφαλίζεται η συμμόρφωση με τις σχετικές πολιτικές.

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Βασικό	Ύπαρξη περιοδικών ανεξάρτητων εσωτερικών ή εξωτερικών ελέγχων με πεδίο εφαρμογής που καλύπτει όλα τα μέρη τα οποία σχετίζονται με τις παρεχόμενες υπηρεσίες ώστε να εξασφαλίζεται η συμμόρφωση με τις σχετικές πολιτικές.
Υψηλό	1. Ύπαρξη περιοδικών ανεξάρτητων εξωτερικών ελέγχων με πεδίο εφαρμογής που καλύπτει όλα τα μέρη τα οποία σχετίζονται με τις παρεχόμενες υπηρεσίες ώστε να εξασφαλίζεται η συμμόρφωση με τις σχετικές πολιτικές. 2. Όταν ένα σχέδιο υπόκειται σε άμεση διαχείριση από δημόσιο φορέα, υπόκειται σε έλεγχο σύμφωνα με την εθνική νομοθεσία.