



#### Περιεχόμενα

#### II Μη νομοθετικές πράξεις

##### ΚΑΝΟΝΙΣΜΟΙ

- \* Εκτελεστικός κανονισμός (ΕΕ) 2015/1501 της Επιτροπής, της 8ης Σεπτεμβρίου 2015, για το πλαίσιο διαλειτουργικότητας σύμφωνα με το άρθρο 12 παράγραφος 8 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 <sup>(1)</sup> ..... 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 <sup>(1)</sup> ..... 7
- Εκτελεστικός κανονισμός (ΕΕ) 2015/1503 της Επιτροπής, της 8ης Σεπτεμβρίου 2015, για καθορισμό των κατ' αποκοπή τιμών εισαγωγής για τον προσδιορισμό της τιμής εισόδου ορισμένων οπωροκηπευτικών ..... 21

##### ΑΠΟΦΑΣΕΙΣ

- \* Εκτελεστική απόφαση (ΕΕ) 2015/1504 της Επιτροπής, της 7ης Σεπτεμβρίου 2015, για τη χορήγηση παρεκκλίσεων σε ορισμένα κράτη μέλη όσον αφορά την υποβολή στατιστικών σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 1099/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις στατιστικές ενέργειας [κοινοποιηθείσα υπό τον αριθμό C(2015) 6105] <sup>(1)</sup> ..... 24
- \* Εκτελεστική απόφαση (ΕΕ) 2015/1505 της Επιτροπής, της 8ης Σεπτεμβρίου 2015, περί καθορισμού των τεχνικών προδιαγραφών και των μορφότυπων των καταλόγων εμπιστευσης σύμφωνα με το άρθρο 22 παράγραφος 5 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 <sup>(1)</sup> ..... 26

<sup>(1)</sup> Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ

- \* Εκτελεστική απόφαση (ΕΕ) 2015/1506 της Επιτροπής, της 8ης Σεπτεμβρίου 2015, για τον καθορισμό προδιαγραφών σχετικά με τους μορφότυπους των προηγμένων ηλεκτρονικών υπογραφών και των προηγμένων σφραγίδων που πρέπει να αναγνωρίζονται από φορείς του δημόσιου τομέα σύμφωνα με τα άρθρα 27 παράγραφος 5 και 37 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά <sup>(1)</sup> .....

---

<sup>(1)</sup> Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ

## II

(Μη νομοθετικές πράξεις)

## ΚΑΝΟΝΙΣΜΟΙ

## ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2015/1501 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 8ης Σεπτεμβρίου 2015

για το πλαίσιο διαλειτουργικότητας σύμφωνα με το άρθρο 12 παράγραφος 8 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<sup>(1)</sup>, και ιδίως το άρθρο 12 παράγραφος 8,

Εκτιμώντας τα ακόλουθα:

- (1) Το άρθρο 12 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014 προβλέπει ότι πρέπει να δημιουργηθεί ένα πλαίσιο διαλειτουργικότητας για τους σκοπούς της διαλειτουργικότητας των εθνικών σχεδίων ηλεκτρονικής ταυτοποίησης που κοινοποιούνται σύμφωνα με το άρθρο 9 παράγραφος 1 του εν λόγω κανονισμού.
- (2) Οι κόμβοι παίζουν κεντρικό ρόλο για τη διασύνδεση των σχεδίων ηλεκτρονικής ταυτοποίησης των κρατών μελών. Η συνεισφορά τους εξηγείται στην τεκμηρίωση σχετικά με τη διευκόλυνση «Συνδέοντας την Ευρώπη» που συστάθηκε βάσει του κανονισμού (ΕΕ) αριθ. 1316/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>(2)</sup>, συμπεριλαμβανομένων των λειτουργιών και συνιστωσών του «κόμβου eIDAS».
- (3) Όταν ένα κράτος μέλος ή η Επιτροπή παρέχει λογισμικό για τη διευκόλυνση επαλήθευσης της ταυτότητας σε έναν κόμβο που λειτουργεί σε άλλο κράτος μέλος, το συμβαλλόμενο μέρος το οποίο παρέχει και επικαιροποιεί το λογισμικό που χρησιμοποιείται για τον μηχανισμό ελέγχου της ταυτότητας μπορεί να συμφωνήσει με το μέρος που φιλοξενεί το λογισμικό όσον αφορά τον τρόπο με τον οποίο θα εξασφαλίζεται η διαχείριση της λειτουργίας του μηχανισμού ελέγχου της ταυτότητας. Μια τέτοια συμφωνία δεν θα πρέπει να επιβάλλει δυσανάλογες τεχνικές απαιτήσεις ή δαπάνες (συμπεριλαμβανομένης της υποστήριξης, των αρμοδιοτήτων, της εξυπηρέτησης και άλλων δαπανών) στο συμβαλλόμενο μέρος εξυπηρέτησης.
- (4) Στον βαθμό που δικαιολογείται από την εφαρμογή του πλαισίου διαλειτουργικότητας, θα μπορούσαν να αναπτυχθούν από την Επιτροπή περαιτέρω τεχνικές προδιαγραφές οι οποίες θα παρέχουν λεπτομέρειες σχετικά με τις τεχνικές απαιτήσεις που προβλέπονται στον παρόντα κανονισμό, σε συνεργασία με τα κράτη μέλη, έχοντας υπόψη ιδίως τις γνωμοδοτήσεις του δικτύου συνεργασίας που αναφέρεται στο άρθρο 14 στοιχείο δ) της εκτελεστικής απόφασης της Επιτροπής (ΕΕ) 2015/296<sup>(3)</sup>. Οι εν λόγω προδιαγραφές θα πρέπει να καταρτιστούν ως μέρος των υποδομών ψηφιακών υπηρεσιών, του κανονισμού (ΕΕ) αριθ. 1316/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, που παρέχει τα μέσα για την πρακτική εφαρμογή ενός δομικού στοιχείου ηλεκτρονικής ταυτοποίησης.

<sup>(1)</sup> ΕΕ L 257 της 28.8.2014, σ. 73.

<sup>(2)</sup> Κανονισμός (ΕΕ) αριθ. 1316/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2013, για τη σύσταση της διευκόλυνσης «Συνδέοντας την Ευρώπη», την τροποποίηση του κανονισμού (ΕΕ) αριθ. 913/2010 και την κατάργηση των κανονισμών (ΕΚ) αριθ. 680/2007 και (ΕΚ) αριθ. 67/2010 (ΕΕ L 348 της 20.12.2013, σ. 129).

<sup>(3)</sup> Εκτελεστική απόφαση (ΕΕ) 2015/296 της Επιτροπής, της 24ης Φεβρουαρίου 2015, για τη θέσπιση διαδικαστικών λεπτομερειών της συνεργασίας μεταξύ των κρατών μελών σχετικά με την ηλεκτρονική ταυτοποίηση σύμφωνα με το άρθρο 12 παράγραφος 7 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 53 της 25.2.2015, σ. 14).

- (5) Οι τεχνικές απαιτήσεις που καθορίζονται στον παρόντα κανονισμό θα πρέπει να εφαρμόζονται παρά τις τυχόν αλλαγές στις τεχνικές προδιαγραφές που θα μπορούσαν να καταρτιστούν σύμφωνα με το άρθρο 12 του παρόντος κανονισμού.
- (6) Κατά τον καθορισμό των ρυθμίσεων του πλαισίου διαλειτουργικότητας που ορίζεται στον παρόντα κανονισμό έχουν ληφθεί ιδιαίτερος υπόψη η πιλοτική εφαρμογή μεγάλης κλίμακας STORK, συμπεριλαμβανομένων των προδιαγραφών που αναπτύσσονται από αυτή, και των αρχών και εννοιών του ευρωπαϊκού πλαισίου διαλειτουργικότητας για τις ευρωπαϊκές δημόσιες υπηρεσίες.
- (7) Τα αποτελέσματα της συνεργασίας μεταξύ των κρατών μελών ελήφθησαν δεόντως υπόψη.
- (8) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 48 του κανονισμού (ΕΕ) αριθ. 910/2014,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

### Άρθρο 1

#### Αντικείμενο

Ο παρών κανονισμός θεσπίζει τις τεχνικές και λειτουργικές απαιτήσεις του πλαισίου διαλειτουργικότητας, ώστε να διασφαλιστεί η διαλειτουργικότητα των σχεδίων ηλεκτρονικής ταυτοποίησης που κοινοποιούν στην Επιτροπή τα κράτη μέλη.

Οι εν λόγω απαιτήσεις περιλαμβάνουν ιδίως:

- α) ελάχιστες τεχνικές απαιτήσεις σχετικά με τα επίπεδα διασφάλισης και τη χαρτογράφηση των εθνικών επιπέδων διασφάλισης των κοινοποιημένων μέσων ηλεκτρονικής ταυτοποίησης που εκδίδονται στο πλαίσιο των κοινοποιημένων σχεδίων ηλεκτρονικής ταυτοποίησης, σύμφωνα με το άρθρο 8 του κανονισμού (ΕΕ) αριθ. 910/2014, όπως ορίζεται στα άρθρα 3 και 4·
- β) ελάχιστες τεχνικές προδιαγραφές για τη διαλειτουργικότητα, όπως ορίζεται στα άρθρα 5 και 8·
- γ) το ελάχιστο σύνολο δεδομένων ταυτοποίησης προσώπου που αντιπροσωπεύουν κατά τρόπο μοναδικό ένα φυσικό ή νομικό πρόσωπο, όπως ορίζεται στο άρθρο 11 και στο παράρτημα·
- δ) κοινά πρότυπα επιχειρησιακής ασφάλειας όπως ορίζονται στα άρθρα 6, 7, 9 και 10·
- ε) ρυθμίσεις για την επίλυση διαφορών όπως ορίζεται στο άρθρο 13.

### Άρθρο 2

#### Ορισμοί

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

- 1) «κόμβος»: το σημείο σύνδεσης που αποτελεί μέρος της αρχιτεκτονικής της διαλειτουργικότητας της ηλεκτρονικής ταυτοποίησης και σχετίζεται με τη διασυνοριακή επαλήθευση της ταυτότητας προσώπων και το οποίο έχει την ικανότητα να αναγνωρίζει και να επεξεργάζεται ή να διαβιβάζει στοιχεία σε άλλους κόμβους, επιτρέποντας τις εθνικές υποδομές ηλεκτρονικής ταυτοποίησης ενός κράτους μέλους να διασυνδέεται με τις εθνικές υποδομές ηλεκτρονικής ταυτοποίησης άλλων κρατών μελών·
- 2) «φορέας εκμετάλλευσης κόμβου»: ο φορέας που είναι υπεύθυνος για τη διασφάλιση ότι ο κόμβος εκτελεί ορθά και αξιόπιστα τις λειτουργίες του, ως σημείο σύνδεσης.

## Άρθρο 3

**Ελάχιστες τεχνικές απαιτήσεις σχετικά με τα επίπεδα διασφάλισης**

Οι ελάχιστες τεχνικές απαιτήσεις σχετικά με τα επίπεδα διασφάλισης καθορίζονται στον εκτελεστικό κανονισμό (ΕΕ) 2015/1502 της Επιτροπής <sup>(1)</sup>.

## Άρθρο 4

**Χαρτογράφηση των εθνικών επιπέδων διασφάλισης**

Η χαρτογράφηση των εθνικών επιπέδων διασφάλισης των κοινοποιημένων σχεδίων ηλεκτρονικής ταυτοποίησης πληροί τις απαιτήσεις που ορίζονται στον εκτελεστικό κανονισμό (ΕΕ) 2015/1502 της Επιτροπής. Τα αποτελέσματα της χαρτογράφησης κοινοποιούνται στην Επιτροπή χρησιμοποιώντας το σχεδιάτυπο κοινοποίησης που ορίζεται στην εκτελεστική απόφαση (ΕΕ) 2015/1505 της Επιτροπής <sup>(2)</sup>.

## Άρθρο 5

**Κόμβοι**

1. Ένας κόμβος σε ένα κράτος μέλος είναι σε θέση να συνδέεται με τους κόμβους των άλλων κρατών μελών.
2. Οι κόμβοι είναι σε θέση να διακρίνουν με τεχνικά μέσα, μεταξύ φορέων του δημόσιου τομέα και άλλων συμβαλλόμενων μερών.
3. Η εφαρμογή από ένα κράτος μέλος των τεχνικών απαιτήσεων που ορίζονται στον παρόντα κανονισμό δεν επιβάλλει δυσανάλογες τεχνικές απαιτήσεις και δαπάνες στα άλλα κράτη μέλη προκειμένου αυτά να διαλειτουργούν με την εφαρμογή που έχει υλοποιήσει το πρώτο κράτος μέλος.

## Άρθρο 6

**Ιδιωτικότητα δεδομένων και εμπιστευτικότητα**

1. Η προστασία της ιδιωτικότητας και της εμπιστευτικότητας των δεδομένων που ανταλλάσσονται και η διατήρηση της ακεραιότητας των δεδομένων μεταξύ των κόμβων εξασφαλίζονται με τη χρήση των βέλτιστων διαθέσιμων τεχνικών λύσεων και πρακτικών προστασίας.
2. Οι κόμβοι δεν αποθηκεύουν προσωπικά δεδομένα, με εξαίρεση για το σκοπό που ορίζεται στο άρθρο 9 παράγραφος 3.

## Άρθρο 7

**Ακεραιότητα και γνησιότητα δεδομένων για την επικοινωνία**

Η επικοινωνία μεταξύ των κόμβων πρέπει να διασφαλίζει την ακεραιότητα και τη γνησιότητα των δεδομένων για να εξασφαλίζεται ότι όλα τα αιτήματα και οι απαντήσεις είναι γνήσια και δεν έχουν παραποιηθεί. Για το σκοπό αυτό, οι κόμβοι χρησιμοποιούν λύσεις που έχουν χρησιμοποιηθεί με επιτυχία όσον αφορά τη χρήση σε διασυνοριακή λειτουργία.

<sup>(1)</sup> 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 (βλέπε σ. 7 της παρούσας Επίσημης Εφημερίδας).

<sup>(2)</sup> Εκτελεστική απόφαση (ΕΕ) 2015/1505 της Επιτροπής, της 8ης Σεπτεμβρίου 2015, περί καθορισμού των τεχνικών προδιαγραφών και των μορφότυπων των καταλόγων εμπιστευσης σύμφωνα με το άρθρο 22 παράγραφος 5 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 (βλέπε σ. 26 της παρούσας Επίσημης Εφημερίδας).

## Άρθρο 8

**Μορφότυπος μηνυμάτων για την επικοινωνία**

Οι κόμβοι χρησιμοποιούν για τη σύνταξη κοινά μορφότυπα μηνυμάτων με βάση τα πρότυπα που έχουν ήδη εφαρμοστεί περισσότερες από μία φορές μεταξύ κρατών μελών, και έχει αποδειχθεί ότι λειτουργούν σε επιχειρησιακό περιβάλλον. Η σύνταξη επιτρέπει:

- α) ορθή επεξεργασία του ελάχιστου συνόλου δεδομένων ταυτοποίησης προσώπου που αντιπροσωπεύουν κατά τρόπο μοναδικό ένα φυσικό ή νομικό πρόσωπο·
- β) ορθή επεξεργασία του επιπέδου διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης·
- γ) διάκριση μεταξύ φορέων του δημόσιου τομέα και άλλων συμβαλλόμενων μερών·
- δ) ευελιξία, ώστε να καλύπτονται οι ανάγκες πρόσθετων χαρακτηριστικών που σχετίζονται με την ταυτοποίηση.

## Άρθρο 9

**Διαχείριση ασφάλειας πληροφοριών και μεταδεδομένων**

1. Ο φορέας εκμετάλλευσης κόμβου κοινοποιεί τα μεταδεδομένα της διαχείρισης του κόμβου με τυποποιημένο μηχανικά επεξεργάσιμο τρόπο και με ασφαλή και αξιόπιστα μέσα.
2. Ανακτώνται αυτόματα τουλάχιστον οι παράμετροι που αφορούν την ασφάλεια.
3. Ο φορέας εκμετάλλευσης κόμβου αποθηκεύει δεδομένα τα οποία, σε περίπτωση συμβάντος, επιτρέπουν την ανασυγκρότηση της ακολουθίας της ανταλλαγής μηνυμάτων για την επιβεβαίωση του τόπου και της φύσης του συμβάντος. Τα δεδομένα αποθηκεύονται για ένα χρονικό διάστημα σύμφωνα με τις εθνικές απαιτήσεις και αποτελούνται τουλάχιστον από τα ακόλουθα στοιχεία:
  - α) ταυτοποίηση κόμβου·
  - β) ταυτοποίηση μηνύματος.
  - γ) ημερομηνία και ώρα μηνύματος.

## Άρθρο 10

**Διασφάλιση των πληροφοριών και πρότυπα ασφάλειας**

1. Οι φορείς εκμετάλλευσης κόμβων οι οποίοι παρέχουν επαλήθευση της ταυτότητας αποδεικνύουν ότι, όσον αφορά τους κόμβους οι οποίοι συμμετέχουν στο πλαίσιο διαλειτουργικότητας, ο κόμβος πληροί τις απαιτήσεις του προτύπου ISO/IEC 27001 μέσω πιστοποίησης, ή μέσω ισοδύναμων μεθόδων αξιολόγησης, ή μέσω της συμμόρφωσης με την εθνική νομοθεσία.
2. Οι φορείς εκμετάλλευσης κόμβων εφαρμόζουν τις ενημερώσεις ασφάλειας κρίσιμης σημασίας χωρίς αδικαιολόγητη καθυστέρηση.

## Άρθρο 11

**Δεδομένα ταυτοποίησης προσώπου**

1. Όταν χρησιμοποιείται σε διασυνοριακό πλαίσιο, ένα ελάχιστο σύνολο δεδομένων ταυτοποίησης προσώπου το οποίο αντιπροσωπεύει κατά τρόπο μοναδικό ένα φυσικό ή νομικό πρόσωπο πρέπει να πληροί τις απαιτήσεις που ορίζονται στο παράρτημα.
2. Όταν χρησιμοποιείται σε διασυνοριακό πλαίσιο, ένα ελάχιστο σύνολο δεδομένων για ένα φυσικό πρόσωπο το οποίο εκπροσωπεί ένα νομικό πρόσωπο πρέπει να περιέχει τον συνδυασμό των χαρακτηριστικών που απαριθμούνται στο παράρτημα για τα φυσικά και νομικά πρόσωπα.
3. Τα δεδομένα διαβιβάζονται με βάση τους αρχικούς χαρακτήρες και, κατά περίπτωση, μεταγράφονται επίσης σε λατινικούς χαρακτήρες.

## Άρθρο 12

**Τεχνικές προδιαγραφές**

1. Όπου δικαιολογείται από τη διαδικασία εφαρμογής του πλαισίου διαλειτουργικότητας, το δίκτυο συνεργασίας που θεσπίστηκε με την εκτελεστική απόφαση (ΕΕ) 2015/296 μπορεί να εκδίδει γνωμοδοτήσεις σύμφωνα με το άρθρο 14 στοιχείο δ) της ίδιας οδηγίας σχετικά με την ανάγκη να αναπτυχθούν τεχνικές προδιαγραφές. Οι εν λόγω τεχνικές προδιαγραφές παρέχουν περαιτέρω λεπτομέρειες σχετικά με τις τεχνικές απαιτήσεις που ορίζονται στον παρόντα κανονισμό.
2. Σύμφωνα με τη γνωμοδότηση που αναφέρεται στην παράγραφο 1, η Επιτροπή, σε συνεργασία με τα κράτη μέλη, καταρτίζει τεχνικές προδιαγραφές ως μέρος των υποδομών των ψηφιακών υπηρεσιών του κανονισμού (ΕΕ) αριθ. 1316/2013.
3. Το δίκτυο συνεργασίας εκδίδει γνωμοδότηση σύμφωνα με το άρθρο 14 στοιχείο δ) του εκτελεστικού κανονισμού (ΕΕ) 2015/296 με την οποία αξιολογεί κατά πόσον και σε ποιο βαθμό οι τεχνικές προδιαγραφές που καταρτίζονται σύμφωνα με την παράγραφο 2 αντιστοιχούν στις ανάγκες οι οποίες εντοπίζονται στη γνωμοδότηση που αναφέρεται στην παράγραφο 1 ή τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό. Μπορεί να συστήσει στα κράτη μέλη να λάβουν υπόψη τις τεχνικές προδιαγραφές κατά την εφαρμογή του πλαισίου διαλειτουργικότητας.
4. Η Επιτροπή παρέχει μια εφαρμογή αναφοράς ως παράδειγμα ερμηνείας των τεχνικών προδιαγραφών. Τα κράτη μέλη μπορούν να εφαρμόζουν την παρούσα εφαρμογή αναφοράς ή να τη χρησιμοποιήσουν ως δείγμα κατά τη δοκιμή άλλων εφαρμογών των τεχνικών προδιαγραφών.

## Άρθρο 13

**Επίλυση διαφορών**

1. Όπου είναι δυνατόν, κάθε διαφορά σχετικά με το πλαίσιο διαλειτουργικότητας επιλύεται από τα ενδιαφερόμενα κράτη μέλη μέσω διαπραγματεύσεων.
2. Αν δεν εξευρεθεί λύση σύμφωνα με την παράγραφο 1, το δίκτυο συνεργασίας που έχει συσταθεί σύμφωνα με το άρθρο 12 της εκτελεστικής απόφασης της Επιτροπής (ΕΕ) 2015/296, είναι αρμόδιο για την επίλυση της διαφοράς σύμφωνα με τον εσωτερικό κανονισμό του.

## Άρθρο 14

**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, 8 Σεπτεμβρίου 2015.

Για την Επιτροπή  
Ο Πρόεδρος  
Jean-Claude JUNCKER

## ΠΑΡΑΡΤΗΜΑ

**Απαιτήσεις σχετικά με το ελάχιστο σύνολο δεδομένων ταυτοποίησης προσώπου τα οποία αντιπροσωπεύουν κατά μοναδικό τρόπο ένα φυσικό ή νομικό πρόσωπο, όπως αναφέρονται στο άρθρο 11****1. Ελάχιστο σύνολο δεδομένων για φυσικό πρόσωπο**

Το ελάχιστο σύνολο δεδομένων για φυσικό πρόσωπο περιλαμβάνει όλα τα ακόλουθα υποχρεωτικά χαρακτηριστικά:

- α) σημερινό/-ά επώνυμο/-α·
- β) σημερινό/-ά όνομα/-τα·
- γ) ημερομηνία γέννησης·
- δ) ένα μοναδικό αναγνωριστικό κωδικό κατασκευασμένο από το αποστέλλον κράτος μέλος σύμφωνα με τις τεχνικές προδιαγραφές για τους σκοπούς της διασυνοριακής αναγνώρισης και ο οποίος είναι όσο το δυνατόν πιο ανθεκτικός στο χρόνο.

Το ελάχιστο σύνολο δεδομένων για ένα φυσικό πρόσωπο πρέπει να περιλαμβάνει ένα ή περισσότερα από τα ακόλουθα επιπλέον χαρακτηριστικά:

- α) όνομα/-τα και επώνυμο/-α κατά τη γέννηση·
- β) τόπο γέννησης·
- γ) σημερινή διεύθυνση·
- δ) φύλο.

**2. Ελάχιστο σύνολο δεδομένων για νομικό πρόσωπο**

Το ελάχιστο σύνολο δεδομένων για νομικό πρόσωπο περιλαμβάνει όλα τα ακόλουθα υποχρεωτικά χαρακτηριστικά:

- α) σημερινή επωνυμία·
- β) ένα μοναδικό αναγνωριστικό κωδικό κατασκευασμένο από το αποστέλλον κράτος μέλος σύμφωνα με τις τεχνικές προδιαγραφές για τους σκοπούς της διασυνοριακής αναγνώρισης και ο οποίος είναι όσο το δυνατόν πιο ανθεκτικός στο χρόνο.

Το ελάχιστο σύνολο δεδομένων για νομικό πρόσωπο πρέπει να περιλαμβάνει ένα ή περισσότερα από τα ακόλουθα επιπλέον χαρακτηριστικά:

- α) σημερινή διεύθυνση·
- β) αριθμό μητρώου ΦΠΑ·
- γ) αριθμό φορολογικού μητρώου·
- δ) τον σχετικό αναγνωριστικό κωδικό του άρθρου 3 παράγραφος 1 της οδηγίας 2009/101/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου <sup>(1)</sup>·
- ε) τον αναγνωριστικό κωδικό νομικής οντότητας (LEI) που αναφέρεται στον εκτελεστικό κανονισμό (ΕΕ) αριθ. 1247/2012 της Επιτροπής <sup>(2)</sup>·
- στ) την καταχώριση και αναγνώριση οικονομικών φορέων (EORI) που αναφέρεται στον εκτελεστικό κανονισμό (ΕΕ) αριθ. 1352/2013 της Επιτροπής <sup>(3)</sup>·
- ζ) τον αριθμό ειδικού φόρου κατανάλωσης που προβλέπεται στο άρθρο 2 παράγραφος 12 του κανονισμού αριθ. 389/2012 του Συμβουλίου <sup>(4)</sup>.

<sup>(1)</sup> Οδηγία 2009/101/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, περί συντονισμού των εγγυήσεων που απαιτούνται στα κράτη μέλη εκ μέρους των εταιρειών, κατά την έννοια του άρθρου 48 δεύτερο εδάφιο της Συνθήκης, για την προστασία των συμφερόντων των εταίρων και των τρίτων, με σκοπό να καταστούν οι εγγυήσεις αυτές ισοδύναμες (ΕΕ L 258 της 1.10.2009, σ. 11).

<sup>(2)</sup> Εκτελεστικός κανονισμός (ΕΕ) αριθ. 1247/2012 της Επιτροπής, της 19ης Δεκεμβρίου 2012, για τη θέσπιση τεχνικών προτύπων όσον αφορά τον μορφότυπο και τη συχνότητα αναφορών συναλλαγών σε αρχεία καταγραφής συναλλαγών σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών (ΕΕ L 352 της 21.12.2012, σ. 20).

<sup>(3)</sup> Εκτελεστικός κανονισμός (ΕΕ) αριθ. 1352/2013 της Επιτροπής, της 4ης Δεκεμβρίου 2013, για την κατάρτιση των εντύπων που προβλέπονται στον κανονισμό (ΕΕ) αριθ. 608/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την τελωνειακή επιβολή των δικαιωμάτων διανοητικής ιδιοκτησίας (ΕΕ L 341 της 18.12.2013, σ. 10).

<sup>(4)</sup> Κανονισμός (ΕΕ) αριθ. 389/2012 του Συμβουλίου, της 2ας Μαΐου 2012, για τη διοικητική συνεργασία στον τομέα των ειδικών φόρων κατανάλωσης και την κατάργηση του κανονισμού (ΕΚ) αριθ. 2073/2004 (ΕΕ L 121 της 8.5.2012, σ. 1).



## 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<sup>(1)</sup>, 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 ιδιαίτερος 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.

<sup>(1)</sup> 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 μέσω 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 πρόεδρος 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 μέσω 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 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	<ol style="list-style-type: none"> <li>1. Διασφάλιση ότι ο αιτών είναι ενήμερος για τους όρους και τις προϋποθέσεις που συνδέονται με τη χρήση των μέσων ηλεκτρονικής ταυτοποίησης.</li> <li>2. Διασφάλιση ότι ο αιτών είναι ενήμερος για τις προτεινόμενες προφυλάξεις ασφαλείας που συνδέονται με τα μέσα ηλεκτρονικής ταυτοποίησης.</li> <li>3. Συλλογή των σχετικών στοιχείων ταυτότητας που απαιτούνται για την απόδειξη και την επαλήθευση της ταυτότητας.</li> </ol>
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	<ol style="list-style-type: none"> <li>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.</li> <li>2. Τα αποδεικτικά στοιχεία μπορούν να θεωρηθούν πραγματικά, ή ότι υφίστανται σύμφωνα με έγκυρη πηγή και τα αποδεικτικά στοιχεία φαίνεται ότι είναι έγκυρα.</li> <li>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.</li> </ol>
Βασικό	<p>Χαμηλό επίπεδο, και πρέπει να πληρούνται μία από τις εναλλακτικές επιλογές που αναφέρονται στα σημεία 1 έως 4:</p> <ol style="list-style-type: none"> <li>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</li> <li>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</li> <li>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 (<sup>1</sup>), ή από ισοδύναμο φορέα.  Ή</li> <li>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 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.</li> </ol>

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Υψηλό	<p>Πρέπει να πληρούνται οι απαιτήσεις των σημείων 1 και 2:</p> <p>1. Βασικό επίπεδο, και πρέπει να πληρούνται μία από τις εναλλακτικές επιλογές που αναφέρονται στα σημεία α έως γ:</p> <p>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·</p> <p>και</p> <p>ο αιτών ταυτοποιείται με τη δηλωθείσα ταυτότητα με σύγκριση ενός ή περισσότερων σωματικών χαρακτηριστικών του προσώπου με έγκυρη πηγή·</p> <p>ή</p> <p>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</p> <p>και</p> <p>λαμβάνονται μέτρα για να αποδειχτεί ότι τα αποτελέσματα των προηγούμενων διαδικασιών εξακολουθούν να ισχύουν·</p> <p>ή</p> <p>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.</p> <p>και</p> <p>λαμβάνονται μέτρα για να αποδειχθεί ότι τα αποτελέσματα της εν λόγω προηγούμενης διαδικασίας έκδοσης του κοινοποιημένου μέσου ηλεκτρονικής ταυτοποίησης εξακολουθούν να ισχύουν.</p> <p>Ή</p> <p>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 καταχώριση όσον αφορά την απόκτηση αναγνωρισμένης φωτογραφίας ή των βιομετρικών στοιχείων ταυτοποίησης.</p>

(<sup>1</sup>) 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	<p>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.</p>

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
	<p>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.</p> <p>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.</p>
Βασικό	<p>Χαμηλό επίπεδο, και πρέπει να πληρούνται μία από τις εναλλακτικές επιλογές που αναφέρονται στα σημεία 1 έως 3:</p> <p>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·</p> <p>και</p> <p>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·</p> <p>και</p> <p>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.</p> <p>Ή</p> <p>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.</p> <p>Ή</p> <p>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.</p>
Υψηλό	<p>Βασικό επίπεδο, και πρέπει να πληρούνται μία από τις εναλλακτικές επιλογές που αναφέρονται στα σημεία 1 έως 3:</p> <p>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·</p> <p>και</p> <p>τα αποδεικτικά στοιχεία ελέγχονται, προκειμένου να διαπιστωθεί ότι είναι γνήσια σύμφωνα με έγκυρη πηγή.</p> <p>Ή</p>

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
	<p>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·</p> <p>και</p> <p>λαμβάνονται μέτρα για να αποδειχτεί ότι τα αποτελέσματα της εν λόγω προηγούμενης διαδικασίας εξακολουθούν να ισχύουν.</p> <p>Ή</p> <p>3. Όταν εκδίδονται μέσα ηλεκτρονικής ταυτοποίησης βάσει έγκυρων κοινοποιημένων μέσω 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·</p> <p>και</p> <p>λαμβάνονται μέτρα για να αποδειχτεί ότι τα αποτελέσματα της εν λόγω προηγούμενης διαδικασίας έκδοσης του κοινοποιημένου μέσου ηλεκτρονικής ταυτοποίησης εξακολουθούν να ισχύουν.</p>

#### 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	<ol style="list-style-type: none"> <li>1. Η εξακρίβωση της ταυτότητας του φυσικού προσώπου που ενεργεί για λογαριασμό του νομικού προσώπου επαληθεύεται ως πραγματοποιηθείσα σε χαμηλό επίπεδο ή ανώτερο.</li> <li>2. Η σύνδεση έχει καθοριστεί σύμφωνα με διαδικασίες αναγνωρισμένες σε εθνικό επίπεδο.</li> <li>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.</li> </ol>
Βασικό	<p>Σημείο 3 χαμηλού επιπέδου, συν:</p> <ol style="list-style-type: none"> <li>1. Η εξακρίβωση της ταυτότητας του φυσικού προσώπου που ενεργεί για λογαριασμό του νομικού προσώπου επαληθεύεται ως πραγματοποιηθείσα σε βασικό ή υψηλό επίπεδο.</li> </ol>



Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
	<p>2. Η σύνδεση καθορίζεται σύμφωνα με διαδικασίες αναγνωρισμένες σε εθνικό επίπεδο, οι οποίες καταλήγουν στην καταχώριση της σύνδεσης σε έγκυρη πηγή.</p> <p>3. Η σύνδεση έχει ελεγχθεί με βάση πληροφορίες από έγκυρη πηγή.</p>
Υψηλό	<p>Σημείο 3 χαμηλού επιπέδου και σημείο 2 βασικού επιπέδου, συν:</p> <p>1. Η εξακρίβωση της ταυτότητας του φυσικού προσώπου που ενεργεί για λογαριασμό του νομικού προσώπου επαληθεύεται ως πραγματοποιηθείσα σε υψηλό επίπεδο.</p> <p>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.</p>

## 2.2. Διαχείριση μέσων ηλεκτρονικής ταυτοποίησης

### 2.2.1. Χαρακτηριστικά και σχεδιασμός μέσων ηλεκτρονικής ταυτοποίησης

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	<p>1. Το μέσο ηλεκτρονικής ταυτοποίησης χρησιμοποιεί τουλάχιστον ένα μέσο επαλήθευσης της ταυτότητας.</p> <p>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.</p>
Βασικό	<p>1. Το μέσο ηλεκτρονικής ταυτοποίησης χρησιμοποιεί τουλάχιστον δύο μέσα επαλήθευσης της ταυτότητας διαφορετικών κατηγοριών.</p> <p>2. Το μέσο ηλεκτρονικής ταυτοποίησης σχεδιάζεται έτσι ώστε να θεωρείται ότι χρησιμοποιείται μόνον υπό τον έλεγχο ή την κατοχή του προσώπου στο οποίο ανήκει.</p>
Υψηλό	<p>Βασικό επίπεδο, συν:</p> <p>1. Το μέσο ηλεκτρονικής ταυτοποίησης προστατεύει έναντι αντιγραφής και παραποίησης καθώς και έναντι επιθέσεων υψηλού κινδύνου</p> <p>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.</p>

### 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	<ol style="list-style-type: none"> <li>Είναι δυνατόν να ανασταλεί και/ή να ανακληθεί ένα μέσο ηλεκτρονικής ταυτοποίησης με έγκαιρο και αποτελεσματικό τρόπο.</li> <li>Υπαρξη μέτρων που λαμβάνονται για την πρόληψη μη εξουσιοδοτημένης αναστολής, ανάκλησης και/ή επανενεργοποίησης.</li> <li>Επανενεργοποίηση πραγματοποιείται μόνο αν συνεχίζουν να πληρούνται οι ίδιες απαιτήσεις διασφάλισης που είχαν καθοριστεί πριν από την αναστολή ή την ανάκληση.</li> </ol>
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	<ol style="list-style-type: none"> <li>Πριν από την ανακοίνωση των στοιχείων ταυτοποίησης προσώπου προηγείται αξιόπιστη επαλήθευση του μέσου ηλεκτρονικής ταυτοποίησης και της ισχύος του.</li> <li>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.</li> <li>Ο μηχανισμός επαλήθευσης της ταυτότητας εφαρμόζει διαδικασίες ελέγχου της ασφάλειας για την επαλήθευση του μέσου ηλεκτρονικής ταυτοποίησης, έτσι ώστε να καταστεί εξαιρετικά απίθανη η υπονόμηση των μηχανισμών επαλήθευσης ταυτότητας από εικασίες, υποκλοπές, αναπαραγωγή ή παραποίηση επικοινωνίας από επιθέσεις ενισχυμένου-βασικού κινδύνου.</li> </ol>

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Βασικό	<p>Χαμηλό επίπεδο, συν:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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 υπονόμηση των μηχανισμών επαλήθευσης ταυτότητας από εικασίες, υποκλοπές, αναπαραγωγή ή παραποίηση επικοινωνίας από επιθέσεις μεσαίου κινδύνου.</li> </ol>
Υψηλό	<p>Βασικό επίπεδο, συν:</p> <p>Ο μηχανισμός επαλήθευσης της ταυτότητας εφαρμόζει διαδικασίες ελέγχου της ασφάλειας για την επαλήθευση του μέσου ηλεκτρονικής ταυτοποίησης, έτσι ώστε να καταστεί εξαιρετικά απίθανη η υπονόμηση των μηχανισμών επαλήθευσης ταυτότητας από εικασίες, υποκλοπές, αναπαραγωγή ή παραποίηση επικοινωνίας από επιθέσεις υψηλού κινδύνου.</p>

#### 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	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> <li>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.</li> <li>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.</li> </ol>
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	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Πρέπει να θεσπιστούν κατάλληλες πολιτικές και διαδικασίες ώστε να εξασφαλιστεί η παροχή πλήρων και ορθών απαντήσεων στα αιτήματα παροχής πληροφοριών.</li> </ol>
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	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>
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	<ol style="list-style-type: none"> <li>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.</li> <li>2. Ύπαρξη επαρκούς προσωπικού και υπεργολάβων για την επαρκή λειτουργία και υποστήριξη της υπηρεσίας σύμφωνα με τις οικείες πολιτικές και διαδικασίες.</li> <li>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.</li> <li>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.</li> </ol>
Βασικό	Ταυτίζεται με το χαμηλό επίπεδο.
Υψηλό	Ταυτίζεται με το χαμηλό επίπεδο.

#### 2.4.6. Τεχνικοί έλεγχοι

Επίπεδο διασφάλισης	Απαιτούμενα στοιχεία
Χαμηλό	<ol style="list-style-type: none"> <li>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.</li> <li>2. Οι δίαυλοι ηλεκτρονικής επικοινωνίας που χρησιμοποιούνται για την ανταλλαγή προσωπικών ή ευαίσθητων πληροφοριών προστατεύονται από υποκλοπές, παραποίηση και αναπαραγωγή.</li> <li>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.</li> <li>4. Υφίστανται διαδικασίες ώστε να διασφαλίζεται διαχρονικά η ασφάλεια και η ικανότητα ανταπόκρισης στις αλλαγές των επιπέδων κινδύνου, στα συμβάντα και στις παραβιάσεις ασφαλείας.</li> <li>5. Όλα τα μέσα που περιλαμβάνουν προσωπικές, κρυπτογραφικές ή άλλες ευαίσθητες πληροφορίες αποθηκεύονται, μεταφέρονται και απορρίπτονται κατά ασφαλή τρόπο.</li> </ol>
Βασικό	<p>Χαμηλό επίπεδο συν:</p> <p>Το ευαίσθητο κρυπτογραφικό υλικό, εάν αυτό χρησιμοποιείται για την έκδοση μέσου ηλεκτρονικής ταυτοποίησης και επαλήθευσης της ταυτότητας προστατεύεται από παρεμβάσεις παραποίησης</p>
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	Υπαρξη 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	<ol style="list-style-type: none"><li data-bbox="469 383 1418 472">1. Υπαρξη 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.</li><li data-bbox="469 483 1418 548">2. Όταν ένα σχέδιο υπόκειται σε άμεση διαχείριση από δημόσιο φορέα, υπόκειται σε έλεγχο σύμφωνα με την εθνική νομοθεσία.</li></ol>

## ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2015/1503 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 8ης Σεπτεμβρίου 2015

για καθορισμό των κατ' αποκοπή τιμών εισαγωγής για τον προσδιορισμό της τιμής εισόδου ορισμένων οπωροκηπευτικών

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) αριθ. 1308/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Δεκεμβρίου 2013, για τη θέσπιση κοινής οργάνωσης των αγορών γεωργικών προϊόντων και την κατάργηση των κανονισμών (ΕΟΚ) αριθ. 922/72, (ΕΟΚ) αριθ. 234/79, (ΕΚ) αριθ. 1037/2001 και (ΕΚ) αριθ. 1234/2007 του Συμβουλίου (1),

Έχοντας υπόψη τον εκτελεστικό κανονισμό (ΕΕ) αριθ. 543/2011 της Επιτροπής, της 7ης Ιουνίου 2011, για τη θέσπιση λεπτομερών κανόνων εφαρμογής του κανονισμού (ΕΚ) αριθ. 1234/2007 του Συμβουλίου όσον αφορά τους τομείς των οπωροκηπευτικών και των μεταποιημένων οπωροκηπευτικών (2), και ιδίως το άρθρο 136 παράγραφος 1,

Εκτιμώντας τα ακόλουθα:

- (1) Ο εκτελεστικός κανονισμός (ΕΕ) αριθ. 543/2011 προβλέπει, κατ' εφαρμογή των αποτελεσμάτων των πολυμερών εμπορικών διαπραγματεύσεων του Γύρου της Ουρουγουάης, τα κριτήρια για τον καθορισμό από την Επιτροπή των κατ' αποκοπή τιμών εισαγωγής από τρίτες χώρες, για τα προϊόντα και τις περιόδους που ορίζονται στο παράρτημα XVI μέρος Α του εν λόγω κανονισμού.
- (2) Η κατ' αποκοπή τιμή εισαγωγής υπολογίζεται κάθε εργάσιμη ημέρα, σύμφωνα με το άρθρο 136 παράγραφος 1 του εκτελεστικού κανονισμού (ΕΕ) αριθ. 543/2011, λαμβανομένων υπόψη των ημερήσιων μεταβλητών στοιχείων. Συνεπώς, ο παρών κανονισμός θα πρέπει να αρχίσει να ισχύει την ημέρα της δημοσίευσής του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

*Άρθρο 1*

Οι κατ' αποκοπή τιμές εισαγωγής που αναφέρονται στο άρθρο 136 του εκτελεστικού κανονισμού (ΕΕ) αριθ. 543/2011 καθορίζονται στο παράρτημα του παρόντος κανονισμού.

*Άρθρο 2*Ο παρών κανονισμός αρχίζει να ισχύει την ημέρα της δημοσίευσής 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,  
εξ ονόματος του Προέδρου,  
Jerzy PLEWA

Γενικός Διευθυντής Γεωργίας και Αγροτικής Ανάπτυξης

(1) ΕΕ L 347 της 20.12.2013, σ. 671.

(2) ΕΕ L 157 της 15.6.2011, σ. 1.

## ΠΑΡΑΡΤΗΜΑ

Οι κατ' αποκοπή τιμές εισαγωγής για τον προσδιορισμό της τιμής εισόδου ορισμένων οπωροκηπευτικών

<i>(ευρώ/100 kg)</i>		
Κωδικός ΣΟ	Κωδικός τρίτων χωρών <sup>(1)</sup>	Κατ' αποκοπή τιμή εισαγωγής
0702 00 00	MA	173,3
	MK	48,7
	XS	41,5
	ZZ	87,8
0707 00 05	MK	76,3
	TR	116,3
	XS	42,0
	ZZ	78,2
0709 93 10	TR	133,1
	ZZ	133,1
0805 50 10	AR	135,9
	BO	135,7
	CL	125,5
	UY	142,2
	ZA	136,9
	ZZ	135,2
	ZZ	135,2
0806 10 10	EG	239,8
	MK	63,9
	TR	129,5
	ZZ	144,4
0808 10 80	AR	188,7
	BR	93,9
	CL	134,4
	NZ	143,4
	US	112,5
	UY	110,5
	ZA	117,6
0808 30 90	ZZ	128,7
	AR	131,9
	CL	100,0
	TR	122,9
	ZA	113,5
	ZZ	117,1
	ZZ	117,1
0809 30 10, 0809 30 90	MK	80,1
	TR	141,7
	ZZ	110,9



(ευρώ/100 kg)

Κωδικός ΣΟ	Κωδικός τρίτων χωρών <sup>(1)</sup>	Κατ' αποκοπή τιμή εισαγωγής
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

<sup>(1)</sup> Ονοματολογία των χωρών που ορίζεται στον κανονισμό (ΕΕ) αριθ. 1106/2012 της Επιτροπής, της 27ης Νοεμβρίου 2012, για την εφαρμογή του κανονισμού (ΕΚ) αριθ. 471/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις κοινοτικές στατιστικές του εξωτερικού εμπορίου με τις τρίτες χώρες, όσον αφορά την επικαιροποίηση της ονοματολογίας των χωρών και εδαφών (ΕΕ L 328 της 28.11.2012, σ. 7). Ο κωδικός «ZZ» αντιπροσωπεύει «άλλες χώρες καταγωγής».

# ΑΠΟΦΑΣΕΙΣ

## ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ (ΕΕ) 2015/1504 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 7ης Σεπτεμβρίου 2015

για τη χορήγηση παρεκκλίσεων σε ορισμένα κράτη μέλη όσον αφορά την υποβολή στατιστικών σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 1099/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις στατιστικές ενέργειας

[κοινοποιηθείσα υπό τον αριθμό C(2015) 6105]

(Τα κείμενα στη γαλλική, ελληνική, εσθονική, ολλανδική και σλοβακική γλώσσα είναι τα μόνα αυθεντικά)

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΚ) αριθ. 1099/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 22ας Οκτωβρίου 2008, για τις στατιστικές ενέργειας <sup>(1)</sup>, και ιδίως το άρθρο 5 παράγραφος 4 και το άρθρο 10 παράγραφος 2,

Εκτιμώντας τα ακόλουθα:

- (1) Σύμφωνα με το άρθρο 5 παράγραφος 4 του κανονισμού (ΕΚ) αριθ. 1099/2008, κατόπιν δεόντως αιτιολογημένου αιτήματος κράτους μέλους, είναι δυνατόν να χορηγούνται παρεκκλίσεις όσον αφορά τα τμήματα των εθνικών στατιστικών η συλλογή των οποίων θα συνεπαγόταν υπερβολικό φόρτο για τους ερωτηθέντες.
- (2) Έχουν υποβληθεί αιτήσεις από το Βέλγιο, την Εσθονία, την Κύπρο και τη Σλοβακία για τη χορήγηση παρεκκλίσεων όσον αφορά την υποβολή λεπτομερών στατιστικών σχετικά με την κατανάλωση ενέργειας στα νοικοκυριά κατά είδος τελικής χρήσης για ορισμένα έτη αναφοράς.
- (3) Οι πληροφορίες που παρασχέθηκαν από τα εν λόγω κράτη μέλη δικαιολογούν τη χορήγηση παρεκκλίσεων.
- (4) Τα μέτρα που προβλέπονται στην παρούσα απόφαση είναι σύμφωνα με τη γνώμη της επιτροπής του ευρωπαϊκού στατιστικού συστήματος,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

### Άρθρο 1

Χορηγούνται οι ακόλουθες παρεκκλίσεις από τις διατάξεις του κανονισμού (ΕΚ) αριθ. 1099/2008:

- 1) Χορηγείται στο Βέλγιο παρέκκλιση από την παραγωγή αποτελεσμάτων για το έτος αναφοράς 2015 για το σημείο 1.2.3 στοιχεία 4.2.1 έως 4.2.5, το σημείο 2.2.3 στοιχεία 4.2.1 έως 4.2.5, το σημείο 3.2.3 στοιχεία 3.1 έως 3.6, το σημείο 4.2.3 στοιχεία 7.2.1 έως 7.2.5 και το σημείο 5.2.4 στοιχεία 4.2.1 έως 4.2.5 του παραρτήματος Β όσον αφορά τις λεπτομερείς στατιστικές σχετικά με την κατανάλωση ενέργειας στα νοικοκυριά κατά είδος τελικής χρήσης (όπως ορίζονται στο σημείο 2.3 στοιχείο 26 «Άλλοι τομείς — Οικιστικός κλάδος» του παραρτήματος Α).

<sup>(1)</sup> ΕΕ L 304 της 14.11.2008, σ. 1.

- 2) Χορηγείται στην Εσθονία παρέκκλιση από την παραγωγή αποτελεσμάτων για τα έτη αναφοράς 2015, 2016 και 2017 για το σημείο 1.2.3 στοιχεία 4.2.1 έως 4.2.5, το σημείο 2.2.3 στοιχεία 4.2.1 έως 4.2.5, το σημείο 3.2.3 στοιχεία 3.1 έως 3.6, το σημείο 4.2.3 στοιχεία 7.2.1 έως 7.2.5 και το σημείο 5.2.4 στοιχεία 4.2.1 έως 4.2.5 του παραρτήματος Β όσον αφορά τις λεπτομερείς στατιστικές σχετικά με την κατανάλωση ενέργειας στα νοικοκυριά κατά είδος τελικής χρήσης (όπως ορίζονται στο σημείο 2.3 στοιχείο 26 «Άλλοι τομείς — Οικιστικός κλάδος» του παραρτήματος Α).
- 3) Χορηγείται στην Κύπρο παρέκκλιση από την παραγωγή αποτελεσμάτων για τα έτη αναφοράς 2015, 2016 και 2017 για το σημείο 1.2.3 στοιχεία 4.2.1 έως 4.2.5, το σημείο 2.2.3 στοιχεία 4.2.1 έως 4.2.5, το σημείο 3.2.3 στοιχεία 3.1 έως 3.6 και το σημείο 5.2.4 στοιχεία 4.2.1 έως 4.2.5 του παραρτήματος Β όσον αφορά τις λεπτομερείς στατιστικές σχετικά με την κατανάλωση ενέργειας στα νοικοκυριά κατά είδος τελικής χρήσης (όπως ορίζονται στο σημείο 2.3 στοιχείο 26 «Άλλοι τομείς — Οικιστικός κλάδος» του παραρτήματος Α).
- 4) Χορηγείται στη Σλοβακία παρέκκλιση από την παραγωγή αποτελεσμάτων για τα έτη αναφοράς 2015 και 2016 για το σημείο 1.2.3 στοιχεία 4.2.1 έως 4.2.5, το σημείο 2.2.3 στοιχεία 4.2.1 έως 4.2.5, το σημείο 3.2.3 στοιχεία 3.1 έως 3.6, το σημείο 4.2.3 στοιχεία 7.2.1 έως 7.2.5 και το σημείο 5.2.4 στοιχεία 4.2.1 έως 4.2.5 του παραρτήματος Β όσον αφορά τις λεπτομερείς στατιστικές σχετικά με την κατανάλωση ενέργειας στα νοικοκυριά κατά είδος τελικής χρήσης (όπως ορίζονται στο σημείο 2.3 στοιχείο 26 «Άλλοι τομείς — Οικιστικός κλάδος» του παραρτήματος Α).

## Άρθρο 2

Η παρούσα απόφαση απευθύνεται στο Βασίλειο του Βελγίου, στη Δημοκρατία της Εσθονίας, στην Κυπριακή Δημοκρατία και στη Σλοβακική Δημοκρατία.

Βρυξέλλες, 7 Σεπτεμβρίου 2015.

Για την Επιτροπή  
Marianne THYSSEN  
Μέλος της Επιτροπής

## ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ (ΕΕ) 2015/1505 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 8ης Σεπτεμβρίου 2015

περί καθορισμού των τεχνικών προδιαγραφών και των μορφότυπων των καταλόγων εμπιστευσης σύμφωνα με το άρθρο 22 παράγραφος 5 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 <sup>(1)</sup>, και ιδίως το άρθρο 22 παράγραφος 5,

Εκτιμώντας τα ακόλουθα:

- (1) Οι κατάλογοι εμπιστευσης είναι ουσιώδεις για την οικοδόμηση εμπιστοσύνης μεταξύ των φορέων της αγοράς εφόσον επισημαίνουν την κατάσταση του παρόχου υπηρεσιών κατά τον χρόνο εσοπτείας.
- (2) Η διασυνοριακή χρήση των ηλεκτρονικών υπογραφών έχει διευκολυνθεί με την απόφαση 2009/767/ΕΚ της Επιτροπής <sup>(2)</sup>, με την οποία έχει επιβληθεί η υποχρέωση στα κράτη μέλη να καταρτίζουν, να τηρούν και να δημοσιεύουν καταλόγους εμπιστευσης συμπεριλαμβανομένων πληροφοριών σχετικά με τους παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό σύμφωνα με την οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου <sup>(3)</sup> και οι οποίοι ελέγχονται και πιστοποιούνται από τα κράτη μέλη.
- (3) Το άρθρο 22 του κανονισμού (ΕΕ) αριθ. 910/2014/ΕΕ προβλέπει την υποχρέωση για τα κράτη μέλη να καταρτίζουν, να τηρούν και να δημοσιεύουν καταλόγους εμπιστευσης, με ασφαλή τρόπο, ηλεκτρονικά υπογεγραμμένους ή σφραγισμένους σε μορφή κατάλληλη για αυτοματοποιημένη επεξεργασία και να κοινοποιούν στην Επιτροπή τους φορείς που είναι αρμόδιοι για την κατάρτιση των εθνικών καταλόγων εμπιστευσης.
- (4) Ένας πάροχος υπηρεσιών εμπιστοσύνης και οι υπηρεσίες εμπιστοσύνης που παρέχει θα πρέπει να θεωρούνται αναγνωρισμένα όταν η κατάσταση αναγνώρισης συνδέεται με τον πάροχο στον κατάλογο εμπιστευσης. Προκειμένου να διασφαλιστεί ότι οι λοιπές υποχρεώσεις που απορρέουν από τον κανονισμό (ΕΕ) αριθ. 910/2014, ιδίως εκείνες που προβλέπονται στα άρθρα 27 και 37, μπορούν εύκολα να πληρούνται από τους παρόχους υπηρεσιών εξ αποστάσεως και με ηλεκτρονικά μέσα και προκειμένου να καλυφθούν οι θεμιτές προσδοκίες των άλλων παρόχων υπηρεσιών πιστοποίησης που δεν εκδίδουν αναγνωρισμένα πιστοποιητικά αλλά παρέχουν υπηρεσίες σχετικά με τις ηλεκτρονικές υπογραφές βάσει της οδηγίας 1999/93/ΕΚ και έχουν καταχωριστεί μέχρι τις 30 Ιουνίου 2016, θα πρέπει να δοθεί η δυνατότητα στα κράτη μέλη να προσθέσουν υπηρεσίες εμπιστοσύνης πέραν των εγκεκριμένων στους καταλόγους εμπιστευσης, σε εθελοντική βάση και σε εθνικό επίπεδο, με την προϋπόθεση ότι θα αναφέρεται σαφώς ότι δεν είναι αναγνωρισμένες σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014.
- (5) Σύμφωνα με την αιτιολογική σκέψη 25 του κανονισμού (ΕΕ) αριθ. 910/2014, τα κράτη μέλη μπορούν να προσθέσουν άλλους τύπους εθνικά καθορισμένων υπηρεσιών εμπιστοσύνης πέραν αυτών που καθορίζονται σύμφωνα με το άρθρο 3 παράγραφος 16 του κανονισμού (ΕΕ) αριθ. 910/2014, με την προϋπόθεση ότι θα αναφέρεται σαφώς ότι δεν είναι αναγνωρισμένες σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014.
- (6) Τα μέτρα που προβλέπονται στην παρούσα απόφαση είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 48 του κανονισμού (ΕΕ) αριθ. 910/2014,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

## Άρθρο 1

Τα κράτη μέλη πρέπει να καταρτίζουν, να δημοσιεύουν και να διατηρούν καταλόγους εμπιστευσης συμπεριλαμβανομένων πληροφοριών σχετικά με τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης τους οποίους επιτηρούν, καθώς και πληροφορίες σχετικά με τις αναγνωρισμένες υπηρεσίες εμπιστοσύνης που παρέχουν. Οι εν λόγω κατάλογοι πρέπει να πληρούν τις τεχνικές προδιαγραφές που ορίζονται στο παράρτημα Ι.

<sup>(1)</sup> ΕΕ L 257 της 28.8.2014, σ. 73.

<sup>(2)</sup> Απόφαση 2009/767/ΕΚ της Επιτροπής, της 16ης Οκτωβρίου 2009, σχετικά με τη θέσπιση μέτρων που διευκολύνουν τη χρήση διαδικασιών με ηλεκτρονικά μέσα μέσω των «ενιαίων κέντρων εξυπηρέτησης» βάσει της οδηγίας 2006/123/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις υπηρεσίες στην εσωτερική αγορά (ΕΕ L 274 της 20.10.2009, σ. 36).

<sup>(3)</sup> Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές (ΕΕ L 13 της 19.1.2000, σ. 12).

### Άρθρο 2

Τα κράτη μέλη μπορούν να συμπεριλάβουν στους καταλόγους εμπιστευσης πληροφορίες σχετικά με μη αναγνωρισμένους παρόχους υπηρεσιών εμπιστοσύνης, καθώς και πληροφορίες σχετικά με τις μη αναγνωρισμένες υπηρεσίες εμπιστοσύνης που παρέχονται από αυτούς. Ο κατάλογος αναφέρει σαφώς τους παρόχους υπηρεσιών εμπιστοσύνης οι οποίοι δεν είναι αναγνωρισμένοι και τις υπηρεσίες εμπιστοσύνης που παρέχονται από αυτούς.

### Άρθρο 3

1. Σύμφωνα με το άρθρο 22 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 910/2014, τα κράτη μέλη πρέπει να υπογράφουν ή να σφραγίζουν ηλεκτρονικά την κατάλληλη για αυτοματοποιημένη επεξεργασία μορφή των καταλόγων εμπιστοσύνης τους σύμφωνα με τις τεχνικές προδιαγραφές που καθορίζονται στο παράρτημα I.
2. Εάν ένα κράτος μέλος δημοσιεύει ηλεκτρονικά μια αναγνώσιμη από άνθρωπο μορφή του καταλόγου εμπιστευσης, μεριμνά ώστε η εν λόγω μορφή του καταλόγου εμπιστευσης να περιέχει τα ίδια δεδομένα με την κατάλληλη για αυτοματοποιημένη επεξεργασία μορφή και να την υπογράφει ή να τη σφραγίζει ηλεκτρονικά σύμφωνα με τις τεχνικές προδιαγραφές που καθορίζονται στο παράρτημα I.

### Άρθρο 4

1. Τα κράτη μέλη κοινοποιούν στην Επιτροπή τις πληροφορίες που αναφέρονται στο άρθρο 22 παράγραφος 3 του κανονισμού (ΕΕ) αριθ. 910/2014, χρησιμοποιώντας το υπόδειγμα του παραρτήματος II.
2. Οι πληροφορίες που αναφέρονται στην παράγραφο 1 περιλαμβάνουν δύο ή περισσότερα πιστοποιητικά δημόσιου κλειδιού του φορέα εκμετάλλευσης του σχεδίου, με μετατιθέμενες περιόδους ισχύος τουλάχιστον τριών μηνών, που αντιστοιχούν στα ιδιωτικά κλειδιά τα οποία μπορούν να χρησιμοποιηθούν για την ηλεκτρονική υπογραφή ή σφράγιση της κατάλληλης για αυτοματοποιημένη επεξεργασία μορφής του καταλόγου εμπιστευσης και της αναγνώσιμης από άνθρωπο μορφής κατά τη δημοσίευσή της.
3. Σύμφωνα με το άρθρο 22 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 910/2014, η Επιτροπή θέτει στη διάθεση του κοινού, μέσω ασφαλούς διαύλου σε επικυρωμένο εξυπηρετητή διαδικτύου, τις πληροφορίες που αναφέρονται στις παραγράφους 1 και 2, όπως κοινοποιήθηκαν από τα κράτη μέλη, με υπογεγραμμένη ή σφραγισμένη μορφή κατάλληλη για αυτοματοποιημένη επεξεργασία.
4. Η Επιτροπή θέτει στη διάθεση του κοινού, μέσω ασφαλούς διαύλου σε έναν επικυρωμένο εξυπηρετητή διαδικτύου, τις πληροφορίες που αναφέρονται στις παραγράφους 1 και 2, όπως κοινοποιήθηκαν από τα κράτη μέλη, με υπογεγραμμένη ή σφραγισμένη μορφή αναγνώσιμη από άνθρωπο.

### Άρθρο 5

Η παρούσα απόφαση αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Η παρούσα απόφαση είναι δεσμευτική ως προς όλα τα μέρη της και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 8 Σεπτεμβρίου 2015.

Για την Επιτροπή  
Ο Πρόεδρος  
Jean-Claude JUNCKER

## ΠΑΡΑΡΤΗΜΑ Ι

## ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΕΝΑ ΚΟΙΝΟ ΣΧΕΔΙΟΤΥΠΟ ΓΙΑ ΤΟΥΣ ΚΑΤΑΛΟΓΟΥΣ ΕΜΠΙΣΤΕΥΣΗΣ

## ΚΕΦΑΛΑΙΟ Ι

## ΓΕΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

Οι κατάλογοι εμπιστευσης περιλαμβάνουν τόσο τις τρέχουσες όσο και όλες τις πληροφορίες σχετικά με το ιστορικό, που χρονολογούνται από την καταχώριση ενός παρόχου υπηρεσιών εμπιστοσύνης στους καταλόγους εμπιστευσης, σχετικά με την κατάσταση των καταγεγραμμένων υπηρεσιών εμπιστοσύνης.

Οι όροι «εγκεκριμένος», «διαπιστευμένος» και/ή «εποπτευόμενος» στις παρούσες προδιαγραφές καλύπτουν επίσης τα εθνικά σχέδια έγκρισης, αλλά θα παρέχονται από τα κράτη μέλη στους οικείους καταλόγους εμπιστευσης πρόσθετες πληροφορίες σχετικά με τη φύση οποιωνδήποτε τέτοιων εθνικών σχεδίων, συμπεριλαμβανομένων διευκρινίσεων σχετικά με τις ενδεχόμενες διαφορές με τα σχέδια εποπτείας που εφαρμόζονται για τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης και τις εγκεκριμένες υπηρεσίες εμπιστοσύνης που παρέχουν.

Οι πληροφορίες που παρέχονται στον κατάλογο εμπιστευσης αποσκοπούν κυρίως στην υποστήριξη της επικύρωσης των αδειοπλασιών αναγνωρισμένων υπηρεσιών εμπιστοσύνης, δηλαδή των φυσικών ή ψηφιακών (λογικών) αντικειμένων που δημιουργούνται ή που εκδίδονται ως αποτέλεσμα της χρήσης αναγνωρισμένης υπηρεσίας εμπιστοσύνης, π.χ. αναγνωρισμένων ηλεκτρονικών υπογραφών/σφραγίδων, προηγμένων ηλεκτρονικών υπογραφών/σφραγίδων που υποστηρίζονται από αναγνωρισμένο πιστοποιητικό, αναγνωρισμένων χρονοσφραγίδων, αναγνωρισμένων αποδεικτικών στοιχείων ηλεκτρονικής παράδοσης κ.λπ.

## ΚΕΦΑΛΑΙΟ ΙΙ

## ΛΕΠΤΟΜΕΡΕΙΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΤΟΝ ΚΟΙΝΟ ΣΧΕΔΙΟΤΥΠΟ ΓΙΑ ΤΟΥΣ ΚΑΤΑΛΟΓΟΥΣ ΕΜΠΙΣΤΕΥΣΗΣ

Οι παρούσες προδιαγραφές βασίζονται στις προδιαγραφές και τις απαιτήσεις που παρατίθενται στο ETSI TS 119 612 v2.1.1 (στο εξής θα αναφέρεται ως ETSI TS 119 612).

Όταν στις παρούσες προδιαγραφές δεν προσδιορίζεται συγκεκριμένη απαίτηση, ισχύουν εξ ολοκλήρου οι απαιτήσεις του ETSI TS 119 612 διατάξεις 5 και 6. Όταν στις παρούσες προδιαγραφές αναφέρονται συγκεκριμένες απαιτήσεις, υπερισχύουν των αντίστοιχων απαιτήσεων του ETSI TS 119 612. Σε περίπτωση αποκλίσεων μεταξύ των παρούσων προδιαγραφών και αυτών του ETSI TS 119 612, υπερισχύουν οι παρούσες προδιαγραφές.

**Όνομα σχεδίου** (διάταξη 5.3.6)

Το πεδίο αυτό υπάρχει υποχρεωτικά και πληροί τις προδιαγραφές του TS 119 612 διάταξη 5.3.6, όπου χρησιμοποιείται η ακόλουθη επωνυμία για το σχέδιο:

«EN\_name\_value» = «Κατάλογος εμπιστευσης ο οποίος περιλαμβάνει πληροφορίες σχετικά με τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης οι οποίοι εποπτεύονται από το κράτος μέλος έκδοσης, καθώς και πληροφορίες σχετικά με τις αναγνωρισμένες υπηρεσίες εμπιστοσύνης που παρέχονται από αυτούς, σύμφωνα με τις σχετικές διατάξεις του κανονισμού (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»

**Πληροφορίες σχεδίου URI** (διάταξη 5.3.7)

Το πεδίο αυτό υπάρχει υποχρεωτικά και πληροί τις προδιαγραφές του TS 119 612 διάταξη 5.3.7, όπου οι «κατάλληλες πληροφορίες για το σχέδιο» θα πρέπει να συμπεριλαμβάνουν τουλάχιστον:

- Εισαγωγικές πληροφορίες που είναι κοινές σε όλα τα κράτη μέλη όσον αφορά το πεδίο εφαρμογής και το πλαίσιο του καταλόγου εμπιστευσης, το υπάρχον σχέδιο εποπτείας και, κατά περίπτωση, το εθνικό σχέδιο/τα εθνικά σχέδια έγκρισης (π.χ. διαπίστευσης). Το κοινό κείμενο που θα χρησιμοποιείται παρατίθεται παρακάτω, όπου η στοιχειοσειρά «[ονομασία του οικείου κράτους μέλους]» αντικαθίσταται από την ονομασία του οικείου κράτους μέλους:

«Ο παρών κατάλογος είναι ο κατάλογος εμπιστευσης ο οποίος περιλαμβάνει πληροφορίες σχετικά με τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης οι οποίοι εποπτεύονται από [ονομασία του οικείου κράτους μέλους], καθώς και πληροφορίες σχετικά με τις αναγνωρισμένες υπηρεσίες εμπιστοσύνης που παρέχονται από αυτούς, σύμφωνα με τις σχετικές διατάξεις του κανονισμού (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.»

Η διασυνοριακή χρήση των ηλεκτρονικών υπογραφών έχει διευκολυνθεί με την απόφαση 2009/767/ΕΚ της Επιτροπής, της 16ης Οκτωβρίου 2009, η οποία όρισε την υποχρέωση για τα κράτη μέλη να καταρτίζουν, να τηρούν και να δημοσιεύουν καταλόγους εμπιστευσης με πληροφορίες σχετικά με τους παρόχους υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό σύμφωνα με την οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, και οι οποίοι εποπτεύονται/διαπιστεύονται από τα κράτη μέλη. Ο παρών κατάλογος εμπιστευσης αποτελεί συνέχεια του καταλόγου εμπιστευσης που συστάθηκε με την απόφαση 2009/767/ΕΚ.».

Οι κατάλογοι εμπιστευσης αποτελούν ουσιώδη στοιχεία για την οικοδόμηση εμπιστοσύνης μεταξύ των φορέων της αγοράς ηλεκτρονικών υπηρεσιών, επιτρέποντας στους χρήστες να καθορίζουν την κατάσταση αναγνώρισης και το ιστορικό κατάστασης των παρόχων υπηρεσιών εμπιστοσύνης και των υπηρεσιών τους.

Οι κατάλογοι εμπιστευσης των κρατών μελών περιλαμβάνουν, τουλάχιστον, τις πληροφορίες που προβλέπονται στα άρθρα 1 και 2 της εκτελεστικής απόφασης της Επιτροπής (ΕΕ) 2015/1505.

Τα κράτη μέλη μπορούν να περιλαμβάνουν στους καταλόγους εμπιστευσης πληροφορίες σχετικά με μη αναγνωρισμένους παρόχους υπηρεσιών εμπιστοσύνης, καθώς και πληροφορίες σχετικά με τις μη αναγνωρισμένες υπηρεσίες εμπιστοσύνης που παρέχονται από αυτούς. Αναφέρεται σαφώς ότι οι εν λόγω πάροχοι ή υπηρεσίες δεν είναι αναγνωρισμένοι, σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014.

Τα κράτη μέλη μπορούν να περιλαμβάνουν στους καταλόγους εμπιστευσης πληροφορίες σχετικά με εθνικά καθορισμένες υπηρεσίες εμπιστοσύνης άλλων τύπων πέραν αυτών που ορίζονται στο άρθρο 3 παράγραφος 16 του κανονισμού (ΕΕ) αριθ. 910/2014. Αναφέρεται σαφώς ότι δεν είναι αναγνωρισμένοι, σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014.

β) Συγκεκριμένες πληροφορίες σχετικά με το υπάρχον σχέδιο/τα υπάρχοντα σχέδια εποπτείας και κατά περίπτωση το εθνικό σχέδιο/τα εθνικά σχέδια έγκρισης (π.χ. διαπίστευσης), ειδικότερα (¹):

- 1) Πληροφορίες σχετικά με το εθνικό σύστημα εποπτείας που ισχύει για τους αναγνωρισμένους και μη αναγνωρισμένους παρόχους υπηρεσιών εμπιστοσύνης και τις αναγνωρισμένες και μη αναγνωρισμένες υπηρεσίες εμπιστοσύνης που αυτοί παρέχουν, όπως ρυθμίζεται από τον κανονισμό (ΕΕ) αριθ. 910/2014.
- 2) Πληροφορίες, κατά περίπτωση, για τα εθνικά σχέδια εθελοντικής διαπίστευσης που ισχύουν για τους παρόχους υπηρεσιών πιστοποίησης που έχουν εκδώσει εγκεκριμένα πιστοποιητικά σύμφωνα με την οδηγία 1999/93/ΕΚ.

Αυτές οι συγκεκριμένες πληροφορίες περιλαμβάνουν, τουλάχιστον, για κάθε υπάρχον προαναφερθέν σχέδιο:

- 1) Γενική περιγραφή.
- 2) Πληροφορίες για τη διαδικασία που ακολουθείται για το εθνικό σύστημα εποπτείας και, κατά περίπτωση, για την έγκριση στο πλαίσιο εθνικού σχεδίου έγκρισης.
- 3) Πληροφορίες σχετικά με τα κριτήρια βάσει των οποίων οι πάροχοι υπηρεσιών εμπιστοσύνης επιτηρούνται, ή, κατά περίπτωση, εγκρίνονται.
- 4) Πληροφορίες σχετικά με τα κριτήρια και τους κανόνες που χρησιμοποιούνται για την επιλογή υπεύθυνων για την εποπτεία/τον έλεγχο και που ορίζουν πώς αυτοί οι υπεύθυνοι αξιολογούν τους παρόχους υπηρεσιών εμπιστοσύνης και τις υπηρεσίες εμπιστοσύνης που παρέχονται από αυτούς.
- 5) Κατά περίπτωση, λοιπά στοιχεία επικοινωνίας και γενικές πληροφορίες που ισχύουν για τη λειτουργία του σχεδίου.

#### **Τύπος σχεδίου/κοινότητα/κανόνες** (διάταξη 5.3.9)

Το πεδίο αυτό υπάρχει και πληροί τις προδιαγραφές του TS 119 612 διάταξη 5.3.9.

Περιλαμβάνει μόνο URI σε αγγλικά του Ηνωμένου Βασιλείου.

(¹) Τα εν λόγω σύνολα πληροφοριών είναι κρίσιμης σημασίας για τα βασισμένα μέρη για την αξιολόγηση της ποιότητας και του επιπέδου ασφαλείας των εν λόγω συστημάτων. Τα εν λόγω σύνολα πληροφοριών παρέχονται σε επίπεδο καταλόγου εμπιστευσης μέσω της χρήσης του παρόντος «URI σχεδίου πληροφοριών» (διάταξη 5.3.7 — πληροφορίες που παρέχει το κράτος μέλος), του «Τύπου σχεδίου/κοινότητα/κανόνες» (διάταξη 5.3.9 — μέσω της χρήσης ενός κειμένου κοινού για όλα τα κράτη μέλη), και της «Πολιτικής/νομικής σημείωσης TSL» (διάταξη 5.3.11 — κείμενο κοινό για όλα τα κράτη μέλη, μαζί με τη δυνατότητα κάθε κράτους μέλους να προσθέτει κείμενα/παραπομπές που να αφορούν ειδικά το εκάστοτε κράτος μέλος). Επιπλέον πληροφορίες σχετικά με τα εν λόγω συστήματα για μη εγκεκριμένες υπηρεσίες εμπιστοσύνης και εθνικά καθορισμένες (εγκεκριμένες) υπηρεσίες εμπιστοσύνης μπορούν να παρέχονται σε επίπεδο υπηρεσίας, κατά περίπτωση και όταν είναι απαραίτητες (π.χ. για να γίνεται διάκριση μεταξύ πολλών επιπέδων ποιότητας/ασφάλειας) μέσω της χρήσης του «URI καθορισμού υπηρεσίας σχεδίου» (διάταξη 5.5.6).

Περιλαμβάνει τουλάχιστον δύο URI:

- 1) Ένα URI κοινό για τους καταλόγους εμπιστευσης όλων των κρατών μελών, το οποίο οδηγεί σε ένα περιγραφικό κείμενο το οποίο ισχύει για όλους τους καταλόγους εμπιστευσης ως εξής:

URI: <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>

Περιγραφικό κείμενο:

#### *«Συμμετοχή σε ένα σχέδιο*

Κάθε κράτος μέλος πρέπει να δημιουργήσει έναν κατάλογο εμπιστευσης ο οποίος να περιλαμβάνει πληροφορίες σχετικά με τους υπό εποπτεία εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης, καθώς και πληροφορίες σχετικά με τις αναγνωρισμένες υπηρεσίες εμπιστοσύνης που παρέχονται από αυτούς, σύμφωνα με τις σχετικές διατάξεις του κανονισμού (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.

Η παρούσα εφαρμογή αυτών των καταλόγων εμπιστευσης πρέπει επίσης να αναφέρεται στον κατάλογο συνδέσμων (δεικτών) προς τον κατάλογο εμπιστευσης κάθε κράτους μέλους, ο οποίος καταρτίζεται από την Ευρωπαϊκή Επιτροπή.

#### *Πολιτική/κανόνες για την αξιολόγηση των καταγεγραμμένων υπηρεσιών*

Τα κράτη μέλη πρέπει να εποπτεύουν τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης που είναι εγκατεστημένοι στην επικράτεια του κράτους μέλους που τους έχει ορίσει σύμφωνα με το κεφάλαιο III του κανονισμού (ΕΕ) αριθ. 910/2014 προκειμένου να διασφαλίζει ότι οι εν λόγω εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης και οι εγκεκριμένες υπηρεσίες εμπιστοσύνης που παρέχουν πληρούν τις απαιτήσεις που θεσπίζει ο κανονισμός.

Οι κατάλογοι εμπιστευσης των κρατών μελών περιλαμβάνουν, τουλάχιστον, τις πληροφορίες που προβλέπονται στα άρθρα 1 και 2 της εκτελεστικής απόφασης της Επιτροπής (ΕΕ) 2015/1505.

Οι κατάλογοι εμπιστευσης περιλαμβάνουν τόσο τις τρέχουσες όσο και τις πληροφορίες σχετικά με το ιστορικό για την κατάσταση των καταγεγραμμένων υπηρεσιών εμπιστοσύνης.

Ο κατάλογος εμπιστευσης κάθε κράτους μέλους πρέπει να παρέχει πληροφορίες σχετικά με το εθνικό σχέδιο εποπτείας και, κατά περίπτωση, το εθνικό σχέδιο/τα εθνικά σχέδια έγκρισης (π.χ. διαπίστευση), στα οποία καταγράφονται οι πάροχοι υπηρεσιών εμπιστοσύνης και οι υπηρεσίες εμπιστοσύνης που παρέχουν.

#### *Ερμηνεία του καταλόγου εμπιστευσης*

Οι γενικές κατευθυντήριες γραμμές χρήσης για τις εφαρμογές, τις υπηρεσίες ή τα προϊόντα που βασίζονται σε έναν κατάλογο εμπιστευσης ο οποίος δημοσιεύεται σύμφωνα με τις διατάξεις του κανονισμού (ΕΕ) αριθ. 910/2014 είναι οι εξής:

Η κατάσταση “αναγνώρισης” μιας υπηρεσίας εμπιστοσύνης προκύπτει από τον συνδυασμό της αξίας του “Αναγνωριστικού τύπου υπηρεσίας” (“Sti”) σε μια καταχώριση υπηρεσίας και την κατάσταση σύμφωνα με την αξία της “Τρέχουσα κατάσταση υπηρεσίας” από την ημερομηνία που υποδεικνύεται στο “Ημερομηνία και ώρα έναρξης της τρέχουσας κατάστασης”. Πληροφορίες ιστορικού για την εν λόγω κατάσταση αναγνώρισης παρέχεται ομοίως, κατά περίπτωση.

Όσον αφορά τους αναγνωρισμένους παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν αναγνωρισμένα πιστοποιητικά για τις ηλεκτρονικές υπογραφές, τις ηλεκτρονικές σφραγίδες και/ή για την επαλήθευση της ταυτότητας ιστοτόπων:

Μια καταχώριση “CA/QC” “Αναγνωριστικό τύπου υπηρεσίας” (“Sti”) [πιθανώς μια καταχώριση CA/QC που αναγνωρίζεται περαιτέρω ότι αποτελεί “RootCA/QC” μέσω της χρήσης της επέκτασης “Επέκταση πληροφοριών υπηρεσίας” (“Sie”) additionalServiceInformation]

— επισημαίνει ότι οποιοδήποτε πιστοποιητικό για οντότητες-τελικούς αποδέκτες που εκδίδεται από ή βάσει του δημόσιου κλειδιού του CA “Ψηφιακού αναγνωριστικού υπηρεσίας” (“Sdi”) και της ονομασίας του CA (και τα δύο δεδομένα CA να θεωρούνται ως άγκυρα εμπιστοσύνης εισροών) αποτελεί ένα αναγνωρισμένο πιστοποιητικό (QC) υπό την προϋπόθεση ότι περιλαμβάνει ένα τουλάχιστον από τα ακόλουθα:

- την οριζόμενη από το id-etsi-qcs-qccompliance id-etsi-qcs ETSI δήλωση (id-etsi-qcs 1),
- την οριζόμενη από το 0.4.0.1456.1.1 (QCP+) ETSI πολιτική πιστοποιητικών OID,



— την οριζόμενη από το 0.4.0.1456.1.2 (QCP) ETSI πολιτική πιστοποιητικών OID,

και υπό τον όρο ότι αυτό θα εξασφαλίζεται από τον φορέα εποπτείας του κράτους μέλους με έγκυρη κατάσταση υπηρεσίας (δηλαδή “υπό εποπτεία”, “εποπτεία υπό αναστολή”, “διαπιστευμένη” ή “αναγνωρισμένη”) για την εν λόγω εγγραφή

- **και EAN** υπάρχουν πληροφορίες “Sie” “Επέκταση προσδιορισμών”, τότε, εκτός από τον παραπάνω εξ ορισμού κανόνα, τα πιστοποιητικά που ορίζονται μέσω της χρήσης πληροφοριών “Sie” “Επέκταση προσδιορισμών”, τα οποία βασίζονται στην αρχή μιας αλληλουχίας φίλτρων που προσδιορίζουν περαιτέρω ένα σύνολο πιστοποιητικών, πρέπει να εξετάζονται σύμφωνα με τους συσχετιζόμενους προσδιοριστές παρέχοντας επιπλέον πληροφορίες όσον αφορά την κατάσταση αναγνώρισης, την “υποστήριξη από SSCD” και/ή το “νομικό πρόσωπο ως υποκείμενο” (π.χ. τα πιστοποιητικά που περιέχουν συγκεκριμένο OID στην επέκταση της πολιτικής πιστοποιητικού και/ή έχουν συγκεκριμένη σχηματομορφή “Χρήσης κλειδιού” και/ή φιλτράρονται μέσω της χρήσης συγκεκριμένης τιμής η οποία εμφανίζεται σε ένα συγκεκριμένο πεδίο ή επέκταση κ.λπ.). Οι προσδιοριστές αυτοί αποτελούν μέρος του παρακάτω συνόλου “προσδιοριστών”, οι οποίοι χρησιμοποιούνται για να επανορθώσουν την έλλειψη πληροφοριών στο αντίστοιχο περιεχόμενο του QC, και οι οποίοι χρησιμοποιούνται αντίστοιχα:
  - για να δηλώσουν το χαρακτήρα του αναγνωρισμένου πιστοποιητικού:
    - “QCStatement”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά είναι αναγνωρισμένα βάσει της οδηγίας 1999/93/EK,
    - “QCForESig”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, είναι αναγνωρισμένο/-α πιστοποιητικό/-ά ηλεκτρονικής υπογραφής βάσει του κανονισμού (ΕΕ) αριθ. 910/2014,
    - “QCForESeal”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, είναι αναγνωρισμένο/-α πιστοποιητικό/-ά ηλεκτρονικής σφραγίδας βάσει του κανονισμού (ΕΕ) αριθ. 910/2014,
    - “QCForWSA”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, είναι αναγνωρισμένο/-α πιστοποιητικό/-ά ηλεκτρονικού ιστότοπου βάσει του κανονισμού (ΕΕ) αριθ. 910/2014,
  - για να δηλώσουν ότι το πιστοποιητικό δεν πρέπει να θεωρείται αναγνωρισμένο:
    - “NotQualified”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά δεν πρέπει να θεωρείται αναγνωρισμένο, και/ή
  - για να δηλώσουν τη φύση της υποστήριξης από SSCD:
    - “QCWithSSCD”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, έχουν το ιδιωτικό τους κλειδί σε ένα SSCD, ή
    - “QCNoSSCD”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, δεν έχουν το ιδιωτικό τους κλειδί σε ένα SSCD, ή
    - “QCSSCDStatusAsInCert”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, δεν περιέχει/-ουν επεξεργασίμες πληροφορίες σχετικά με το εάν έχουν ή όχι το ιδιωτικό τους κλειδί σε ένα SSCD,
  - για να δηλώσουν τη φύση της υποστήριξης από QSCD:
    - “QCWithQSCD”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, έχουν το ιδιωτικό τους κλειδί σε ένα QSCD, ή
    - “QCNoQSCD”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, δεν έχουν το ιδιωτικό τους κλειδί σε ένα QSCD, ή
    - “QCQSCDStatusAsInCert”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, δεν περιέχει/-ουν επεξεργασίμες πληροφορίες σχετικά με το εάν έχουν ή όχι το ιδιωτικό τους κλειδί σε ένα QSCD,
    - “QCQSCDManagedOnBehalf”, που αναφέρει ότι όλα τα πιστοποιητικά που προσδιορίζονται από τον ισχύοντα κατάλογο κριτηρίων, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένα, έχουν το ιδιωτικό τους κλειδί σε ένα QSCD, για το οποίο η παραγωγή και η διαχείριση του αντίστοιχου ηλεκτρονικού κλειδιού επιτυγχάνονται με αναγνωρισμένο TSP εξ ονόματος της οντότητας της οποίας η ταυτότητα έχει πιστοποιηθεί στο πιστοποιητικό, και/ή

- για να δηλώσουν έκδοση υπέρ νομικού προσώπου:
  - “QCForLegalPerson”, που σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά, όταν δηλώνονται ή αναφέρονται ως αναγνωρισμένο/-α πιστοποιητικό/-ά, εκδίδονται υπέρ νομικού προσώπου βάσει της οδηγίας 1999/93/ΕΚ.

*Σημείωση:* Οι πληροφορίες που παρέχονται στον κατάλογο εμπιστευσης πρέπει να θεωρούνται ακριβείς, με την έννοια ότι:

- εάν δεν περιλαμβάνονται πληροφορίες id-etsi-qcs 1 statement, QCP OID ή QCP+ OID σε ένα πιστοποιητικό για οντότητες-τελικούς αποδέκτες, και
- εάν δεν είναι παρούσες πληροφορίες “Sie” “Επέκταση προσδιορισμών” για την άγκυρα εμπιστοσύνης CA/QC της αντίστοιχης καταχώρισης υπηρεσίας για να αναγνωρίσει το πιστοποιητικό με προσδιοριστή “QCStatement”, ή
- υπάρχουν πληροφορίες “Sie” “Επέκταση προσδιορισμών” για την άγκυρα εμπιστοσύνης CA/QC της αντίστοιχης καταχώρισης υπηρεσίας για να αναγνωρίσει το πιστοποιητικό με προσδιοριστή “notqualified”, τότε το πιστοποιητικό δεν πρέπει να θεωρείται αναγνωρισμένο.

Τα “ψηφιακά αναγνωριστικά υπηρεσίας” πρέπει να χρησιμοποιούνται ως άγκυρες εμπιστοσύνης στο πλαίσιο της επικύρωσης των ηλεκτρονικών υπογραφών ή σφραγίδων για τα οποία το πιστοποιητικό του υπογράφοντα ή του δημιουργού σφραγίδας επικυρώνεται βάση πληροφοριών TL, και ως εκ τούτου μόνο το δημόσιο κλειδί και το όνομα συναφούς θέματος απαιτούνται ως πληροφορίες άγκυρας εμπιστοσύνης. Όταν περισσότερα του ενός πιστοποιητικά εκπροσωπούν το δημόσιο κλειδί για την αναγνώριση της υπηρεσίας, πρέπει να θεωρηθούν ως άγκυρα εμπιστοσύνης πιστοποιητικά άγκυρας εμπιστοσύνης τα οποία αποδίδουν τις ίδιες ακριβώς πληροφορίες όσον αφορά τις πληροφορίες που είναι απόλυτα αναγκαίες ως πληροφορίες άγκυρας εμπιστοσύνης.

Ο γενικός κανόνας ερμηνείας για οποιαδήποτε άλλη καταχώριση τύπου “Sti” είναι ότι, για τον συγκεκριμένο αναγνωρισμένο τύπο υπηρεσίας “Sti”, η καταγεγραμμένη υπηρεσία που ονομάζεται βάσει της τιμής πεδίου “ονομασία υπηρεσίας” και που αναγνωρίζεται κατά μονοσήμαντο τρόπο βάσει της τιμής πεδίου “ψηφιακή ταυτότητα υπηρεσίας” έχει την τρέχουσα κατάσταση έγκρισης ή αναγνώρισης σύμφωνα με την τιμή πεδίου “τρέχουσα κατάσταση υπηρεσίας” από την ημερομηνία που υποδεικνύεται στο “Ημερομηνία και ώρα έναρξης της τρέχουσας κατάστασης”.

Ενδέχεται να εντοπιστούν ειδικοί κανόνες ερμηνείας για οποιεσδήποτε επιπλέον πληροφορίες όσον αφορά μια καταγεγραμμένη υπηρεσία (π.χ. πεδίο “Επεκτάσεις πληροφοριών υπηρεσίας”, κατά περίπτωση, στο ειδικό URI ανά κράτος μέλος, ως μέρος του υπάρχοντος πεδίου “Τύπος/κοινότητες/κανόνες σχεδίου”.

Παρακαλείσθε να συμβουλευθείτε το εφαρμοστέο παράγωγο δίκαιο, σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 910/2014, για περαιτέρω λεπτομέρειες σχετικά με τα πεδία, την περιγραφή και την έννοια των καταλόγων εμπιστευσης των κρατών μελών.».

- 2) Ένα URI ειδικά για τον κατάλογο εμπιστευσης κάθε κράτους μέλους, το οποίο οδηγεί σε ένα περιγραφικό κείμενο το οποίο ισχύει για τον TL του εν λόγω κράτους μέλους:

<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC> όπου CC = ο κωδικός χώρας ISO 3166-1 (!) με δυο αλφαβητικούς χαρακτήρες που χρησιμοποιείται στο πεδίο «Επικράτεια σχεδίου» (διάταξη 5.3.10)

- Σε περιπτώσεις κατά τις οποίες οι χρήστες μπορούν να λάβουν τη συγκεκριμένη πολιτική/τους κανόνες του εκάστοτε κράτους μέλους έναντι των οποίων αξιολογούνται οι υπηρεσίες εμπιστοσύνης που συμπεριλαμβάνονται στον κατάλογο, σύμφωνα με το καθεστώς εποπτείας και, κατά περίπτωση, το σχέδιο έγκρισης του κράτους μέλους.
- Σε περιπτώσεις κατά τις οποίες οι χρήστες μπορούν να λάβουν τη συγκεκριμένη περιγραφή του εκάστοτε κράτους μέλους σχετικά με το πώς να χρησιμοποιήσουν και να ερμηνεύσουν το περιεχόμενο του καταλόγου εμπιστευσης όσον αφορά τις καταγεγραμμένες μη αναγνωρισμένες υπηρεσίες εμπιστοσύνης και/ή τις εθνικά προσδιορισμένες υπηρεσίες εμπιστοσύνης. Αυτό μπορεί να χρησιμοποιηθεί για να δηλώσει πιθανή λεπτομερή ανάλυση του εθνικού συστήματος έγκρισης που σχετίζεται με τους CSP που δεν εκδίδουν QC και το πώς χρησιμοποιούνται για τον σκοπό αυτό τα πεδία «URI καθορισμού υπηρεσίας σχεδίου» (διάταξη 5.5.6) και «επέκταση πληροφοριών υπηρεσίας» (διάταξη 5.5.9).

Τα κράτη μέλη ΔΥΝΑΝΤΑΙ ΝΑ ορίσουν και να χρησιμοποιούν πρόσθετα URI επεκτείνοντας το παραπάνω αποκλειστικό ανά κράτος μέλος URI (δηλαδή, URI τα οποία καθορίζονται από αυτό το ιεραρχικά αποκλειστικό URI).

#### **Πολιτική/νομική σημείωση TSL (διάταξη 5.3.11)**

Το πεδίο αυτό υπάρχει και πληροί με τις προδιαγραφές του TS 119 612 διάταξη 5.3.11, όπου η πολιτική/νομική σημείωση σχετικά με το νομικό καθεστώς του σχεδίου ή τις νομικές απαιτήσεις που πληροί το σχέδιο στη δικαιοδοσία στην οποία είναι εγκατεστημένο και/ή τυχόν περιορισμούς και όρους βάσει των οποίων ο κατάλογος εμπιστευσης τηρείται και δημοσιεύεται είναι

(!) ISO 3166-1:2006: «Κωδικοί ονομάτων χωρών και υποδιαιρέσεών τους — Μέρος 1: Κωδικοί χωρών»

για ακολουθία πολύγλωσσων στοιχειοσειρών (βλέπε διάταξη 5.1.4) η οποία παρέχει, με υποχρεωτική γλώσσα τα αγγλικά του Ηνωμένου Βασιλείου και ενδεχομένως μία ή περισσότερες εθνικές γλώσσες, το πραγματικό κείμενο οποιασδήποτε τέτοιας πολιτικής ή ανακοίνωσης και δομείται ως εξής:

- 1) Ένα πρώτο υποχρεωτικό μέρος, κοινό για τους καταλόγους εμπιστευσης όλων των κρατών μελών σχετικά με το εφαρμοστέο νομικό πλαίσιο και του οποίου η απόδοση στην αγγλική γλώσσα είναι η ακόλουθη:

The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Κείμενο στην εθνική/-ές γλώσσα/-ες του κράτους μέλους:

Το ισχύον νομικό πλαίσιο για τον παρόντα κατάλογο εμπιστευσης είναι ο κανονισμός (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.

- 2) Ένα δεύτερο, προαιρετικό μέρος, ειδικό για κάθε κατάλογο εμπιστευσης, το οποίο περιέχει παραπομπές σε συγκεκριμένα ισχύοντα εθνικά νομικά πλαίσια

### **Τρέχουσα κατάσταση υπηρεσίας** (διάταξη 5.5.4)

Το πεδίο αυτό υπάρχει και πληροί τις προδιαγραφές του TS 119 612 διάταξη 5.5.4.

Η μετακίνηση της τιμής «Τρέχουσα κατάσταση υπηρεσίας» των υπηρεσιών που απαριθμούνται στον κατάλογο εμπιστευσης του EUMS κατά την ημέρα πριν από την ημερομηνία εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 (δηλαδή την 30ή Ιουνίου 2016) πρέπει να εκτελείται από την ημερομηνία κατά την οποία ο εφαρμόζεται ο κανονισμός (δηλαδή την 1η Ιουλίου 2016), όπως ορίζεται στο παράρτημα I του ETSI TS 119 612.

## ΚΕΦΑΛΑΙΟ III

### ΣΥΝΕΧΕΙΑ ΤΩΝ ΚΑΤΑΛΟΓΩΝ ΕΜΠΙΣΤΕΥΣΗΣ

Τα πιστοποιητικά που πρόκειται να κοινοποιηθούν στην Επιτροπή σύμφωνα με το άρθρο 4 παράγραφος 2 της παρούσας απόφασης πληρούν τις απαιτήσεις της διάταξης 5.7.1 του ETSI TS 119 612 και εκδίδονται κατά τέτοιον τρόπο ώστε να:

- έχουν τουλάχιστον τρίμηνη διαφορά κατά την ημερομηνία λήξης ισχύος τους («όχι μετά»),
- δημιουργούνται με βάση νέα ζεύγη κλειδιών. Τα ζεύγη κλειδιών που έχουν χρησιμοποιηθεί κατά το παρελθόν δεν πρέπει να επαναπιστοποιούνται.

Σε περίπτωση λήξης ενός από τα πιστοποιητικά δημόσιου κλειδιού που θα μπορούσε να χρησιμοποιηθεί για την επικύρωση της υπογραφής ή της σφραγίδας του καταλόγου εμπιστευσης που έχει κοινοποιηθεί στην Επιτροπή και δημοσιευθεί στους κεντρικούς καταλόγους δεικτών της Επιτροπής, τα κράτη μέλη:

- σε περίπτωση που ο δημοσιευμένος κατάλογος εμπιστευσης υπογράφηκε ή σφραγίστηκε με ένα ιδιωτικό κλειδί του οποίου το πιστοποιητικό δημόσιου κλειδιού έχει λήξει, επανεκδίδουν, χωρίς καθυστέρηση, νέο κατάλογο εμπιστευσης υπογεγραμμένο ή σφραγισμένο με ένα ιδιωτικό κλειδί του οποίου το κοινοποιημένο πιστοποιητικό δημόσιου κλειδιού δεν έχει λήξει,
- εφόσον απαιτείται, δημιουργούν νέα ζεύγη κλειδιών που θα μπορούσαν να χρησιμοποιηθούν για την υπογραφή ή σφράγιση του καταλόγου εμπιστευσης και αναλαμβάνουν τη δημιουργία των αντίστοιχων πιστοποιητικών δημόσιου κλειδιού,
- ενημερώνουν άμεσα την Επιτροπή για τον νέο κατάλογο πιστοποιητικών δημόσιων κλειδιών που αντιστοιχούν στα ιδιωτικά κλειδιά που θα μπορούσαν να χρησιμοποιηθούν για την υπογραφή ή σφράγιση του καταλόγου εμπιστευσης.

Σε περίπτωση παραβίασης ή κατάργησης ενός από τα ιδιωτικά κλειδιά που αντιστοιχούν σε ένα από τα πιστοποιητικά δημόσιου κλειδιού το οποίο θα μπορούσε να χρησιμοποιηθεί για την επικύρωση της υπογραφής ή της σφράγισης του καταλόγου εμπιστευσης που έχει κοινοποιηθεί στην Επιτροπή και δημοσιευτεί στους κεντρικούς καταλόγους δεικτών της Επιτροπής, τα κράτη μέλη:

- επανεκδίδουν, χωρίς καθυστέρηση, νέο κατάλογο εμπιστευσης υπογεγραμμένο ή σφραγισμένο με το μη παραβιασμένο ιδιωτικό κλειδί σε περιπτώσεις όπου ο δημοσιευμένος κατάλογος εμπιστευσης υπογράφηκε ή σφραγίστηκε με παραβιασμένο ή καταργημένο ιδιωτικό κλειδί,

- εφόσον απαιτείται, δημιουργούν νέα ζεύγη κλειδιών που θα μπορούσαν να χρησιμοποιηθούν για την υπογραφή ή σφράγιση του καταλόγου εμπιστευσης και αναλαμβάνουν τη δημιουργία των αντίστοιχων πιστοποιητικών δημόσιου κλειδιού,
- ενημερώνουν άμεσα την Επιτροπή για τον νέο κατάλογο πιστοποιητικών δημόσιου κλειδιού που αντιστοιχούν στα ιδιωτικά κλειδιά που θα μπορούσαν να χρησιμοποιηθούν για την υπογραφή ή σφράγιση του καταλόγου εμπιστευσης.

Σε περίπτωση παραβίασης ή κατάργησης όλων των ιδιωτικών κλειδιών που αντιστοιχούν στα πιστοποιητικά δημόσιου κλειδιού που θα μπορούσαν να χρησιμοποιηθούν για την επικύρωση της υπογραφής του καταλόγου εμπιστευσης και έχουν κοινοποιηθεί στην Επιτροπή και δημοσιευθεί στους κεντρικούς καταλόγους δεικτών της Επιτροπής, τα κράτη μέλη:

- δημιουργούν νέα ζεύγη κλειδιών που θα μπορούσαν να χρησιμοποιηθούν για την υπογραφή ή σφράγιση του καταλόγου εμπιστευσης και αναλαμβάνουν τη δημιουργία των αντίστοιχων πιστοποιητικών δημόσιου κλειδιού,
- επανεκδίδουν, χωρίς καθυστέρηση, νέο κατάλογο εμπιστευσης υπογεγραμμένο ή σφραγισμένο με ένα από αυτά τα νέα ιδιωτικά κλειδιά και του οποίου το αντίστοιχο πιστοποιητικό δημόσιου κλειδιού πρόκειται να κοινοποιηθεί,
- ενημερώνουν άμεσα την Επιτροπή για τον νέο κατάλογο πιστοποιητικών δημόσιου κλειδιού που αντιστοιχούν στα ιδιωτικά κλειδιά που θα μπορούσαν να χρησιμοποιηθούν για την υπογραφή ή σφράγιση του καταλόγου εμπιστευσης.

#### ΚΕΦΑΛΑΙΟ IV

##### ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΤΗΝ ΑΝΑΓΝΩΣΙΜΗ ΑΠΟ ΑΝΘΡΩΠΟ ΜΟΡΦΗ ΤΟΥ ΚΑΤΑΛΟΓΟΥ ΕΜΠΙΣΤΕΥΣΗΣ

Όταν δημιουργείται και δημοσιεύεται μια αναγνώσιμη από άνθρωπο μορφή του καταλόγου εμπιστευσης, παρέχεται με τη μορφή εγγράφου Portable Document Format (PDF) σύμφωνα με το ISO 32000 <sup>(1)</sup>, το οποίο μορφοποιείται σύμφωνα με το προφίλ PDF/A (ISO 19005 <sup>(2)</sup>).

Το περιεχόμενο μιας αναγνώσιμης από άνθρωπο μορφής βάσει PDF/A του καταλόγου εμπιστευσης πληροί τις παρακάτω απαιτήσεις:

- Η δομή της αναγνώσιμης από άνθρωπο μορφής αντιστοιχεί στο λογικό μοντέλο που περιγράφεται στο TS 119 612.
- Κάθε υπάρχον πεδίο προβάλλεται και παρέχει:
  - τον τίτλο του πεδίου (π.χ. «Αναγνωριστικό τύπου υπηρεσίας»),
  - την τιμή του πεδίου (π.χ. «<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>»),
  - την έννοια (περιγραφή) της τιμής του πεδίου, κατά περίπτωση (π.χ. «Μια υπηρεσία δημιουργίας πιστοποιητικών η οποία δημιουργεί και υπογράφει αναγνωρισμένα πιστοποιητικά με βάση την ταυτότητα και τα λοιπά χαρακτηριστικά που επαληθεύονται από τις αρμόδιες υπηρεσίες καταχώρισης.»),
  - πολλαπλές εκδόσεις σε διάφορες εθνικές γλώσσες, όπως προβλέπεται στον κατάλογο εμπιστευσης, κατά περίπτωση.
- Τα παρακάτω πεδία και οι αντίστοιχες τιμές των ψηφιακών πιστοποιητικών <sup>(3)</sup>, εάν υπάρχουν στο πεδίο «Ψηφιακή ταυτότητα υπηρεσίας» εμφανίζονται τουλάχιστον στην αναγνώσιμη από άνθρωπο μορφή:
  - Έκδοση
  - Αύξων αριθμός πιστοποιητικού
  - Αλγόριθμος υπογραφής
  - Εκδότης — όλα τα συναφή διαχωριζόμενα πεδία ονομασιών
  - Περίοδος ισχύος
  - Θέμα — όλα τα συναφή διαχωριζόμενα πεδία ονομασιών

<sup>(1)</sup> ISO 32000-1:2008: Διαχείριση εγγράφων — Μορφή φορητού εγγράφου — Μέρος 1: PDF 1.7

<sup>(2)</sup> ISO 19005-2:2011: Διαχείριση εγγράφων — Ηλεκτρονική μορφή αρχείου του εγγράφου για μακροχρόνια διατήρηση — Μέρος 2: Χρήση του ISO 32000-1 (PDF/A-2)

<sup>(3)</sup> Σύσταση ITU-T X.509 | ISO/IEC 9594-: Τεχνολογία πληροφοριών — Διασύνδεση ανοιχτών συστημάτων — κατάλογος: Πλαίσια δημόσιου κλειδιού και χαρακτηριστικών πιστοποιητικού (βλέπε <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>)

- Δημόσιο κλειδί
  - Αναγνωριστικό κλειδιού αρχής
  - Αναγνωριστικό κλειδιού υποκειμένου
  - Χρήση κλειδιού
  - Εκτεταμένη χρήση κλειδιού
  - Πολιτικές πιστοποιητικού — όλα τα αναγνωριστικά πολιτικής και οι προσδιοριστές πολιτικής
  - Χαρτογράφηση των πολιτικών
  - Εναλλακτική ονομασία θέματος
  - Χαρακτηριστικά καταλόγου θέματος
  - Βασικοί περιορισμοί
  - Περιορισμοί που αφορούν την πολιτική
  - Σημεία διανομής CRL <sup>(1)</sup>
  - Πρόσβαση σε πληροφορίες αρχών
  - Πρόσβαση σε πληροφορίες θέματος
  - Δηλώσεις Αναγνωρισμένου Πιστοποιητικού <sup>(2)</sup>
  - Αλγόριθμος κατακερματισμού
  - Τιμή κατακερματισμού του πιστοποιητικού
- Η αναγνώσιμη από άνθρωπο μορφή είναι εύκολα εκτυπώσιμη.
- Η αναγνώσιμη από άνθρωπο μορφή είναι υπογεγραμμένη ή σφραγισμένη από τον φορέα εκμετάλλευσης σχεδίου, σύμφωνα με προηγμένη υπογραφή PDF που προσδιορίζεται στα άρθρα 1 και 3 της εκτελεστικής απόφασης της Επιτροπής (ΕΕ) 2015/1505.

---

<sup>(1)</sup> RFC 5280: Διαδικτυακό πιστοποιητικό X.509 υποδομής δημόσιου κλειδιού και Χαρακτηριστικά του CRL

<sup>(2)</sup> RFC 3739: Διαδικτυακή υποδομή δημόσιου κλειδιού X.509: Προφίλ Αναγνωρισμένων Πιστοποιητικών

## ΠΑΡΑΡΤΗΜΑ II

## ΥΠΟΔΕΙΓΜΑ ΓΙΑ ΤΙΣ ΚΟΙΝΟΠΟΙΗΣΕΙΣ ΤΩΝ ΚΡΑΤΩΝ ΜΕΛΩΝ

Οι πληροφορίες που πρέπει να κοινοποιούνται από τα κράτη μέλη σύμφωνα με το άρθρο 4 παράγραφος 1 της παρούσας απόφασης περιέχουν τα ακόλουθα δεδομένα και οποιαδήποτε μεταβολή τους:

- 1) Κράτος μέλος, με χρήση διψήφιων αλφαβητικών κωδικών ISO 3166-1 <sup>(1)</sup> με τις ακόλουθες εξαιρέσεις:
  - α) Ο κωδικός χώρας για το Ηνωμένο Βασίλειο, «UK».
  - β) Ο κωδικός χώρας για την Ελλάδα, «EL».
- 2) Ο φορέας/οι φορείς που είναι αρμόδιος/αρμόδιοι για την κατάρτιση, την τήρηση και τη δημοσίευση της κατάλληλης για αυτοματοποιημένη επεξεργασία μορφής και της αναγνώσιμης από άνθρωπο μορφής των καταλόγων εμπιστευσης:
  - α) Ονομασία φορέα εκμετάλλευσης του σχεδίου: οι παρεχόμενες πληροφορίες πρέπει να είναι πανομοιότυπες — πεζά ή κεφαλαία — στην τιμή «Ονομασία φορέα εκμετάλλευσης του σχεδίου» στον κατάλογο εμπιστευσης σε όσες γλώσσες χρησιμοποιούνται στον κατάλογο εμπιστευσης.
  - β) Προαιρετικές πληροφορίες για εσωτερική χρήση της Επιτροπής μόνο σε περιπτώσεις κατά τις οποίες πρέπει να ενημερωθεί η αρμόδια αρχή (οι πληροφορίες δεν θα δημοσιεύονται στον ενωσιακό συγκεντρωτικό κατάλογο των καταλόγων εμπιστευσης):
    - διεύθυνση του φορέα εκμετάλλευσης του σχεδίου,
    - στοιχεία επικοινωνίας του/των υπεύθυνου/-ων προσώπου/-ων (ονοματεπώνυμο, αριθμός τηλεφώνου, διεύθυνση ηλεκτρονικού ταχυδρομείου).
- 3) Τόπος στον οποίο δημοσιεύεται ο κατάλογος εμπιστευσης υπό μορφή κατάλληλη για αυτοματοποιημένη επεξεργασία (τόπος δημοσίευσης του τρέχοντος καταλόγου εμπιστευσης).
- 4) Τόπος, κατά περίπτωση, στον οποίο δημοσιεύεται ο κατάλογος εμπιστευσης υπό μορφή αναγνώσιμη από άνθρωπο (τόπος δημοσίευσης του τρέχοντος καταλόγου εμπιστευσης). Σε περίπτωση που ένας κατάλογος εμπιστευσης υπό μορφή αναγνώσιμη από άνθρωπο δεν δημοσιεύεται πλέον, γίνεται σχετική μνεία.
- 5) Τα πιστοποιητικά δημόσιου κλειδιού που αντιστοιχούν στα ιδιωτικά κλειδιά τα οποία μπορούν να χρησιμοποιηθούν για την ηλεκτρονική υπογραφή ή σφράγιση της κατάλληλης για αυτοματοποιημένη επεξεργασία μορφής του καταλόγου εμπιστευσης και της αναγνώσιμης από άνθρωπο μορφής των καταλόγων εμπιστευσης: Τα εν λόγω πιστοποιητικά πρέπει να παρέχονται ως πιστοποιητικά DER κωδικοποιημένα με Privacy Enhanced Mail Base64. Για κοινοποίηση τροποποίησης, συμπληρωματικές πληροφορίες σε περίπτωση που ένα νέο πιστοποιητικό πρόκειται να αντικαταστήσει ένα ειδικό πιστοποιητικό στον κατάλογο της Επιτροπής και σε περίπτωση που το κοινοποιηθέν πιστοποιητικό πρόκειται να προστεθεί στο υπάρχον/στα υπάρχοντα, χωρίς να αντικατασταθεί.
- 6) Ημερομηνία υποβολής των δεδομένων που κοινοποιούνται στα σημεία 1 έως 5.

Τα δεδομένα που κοινοποιούνται σύμφωνα με το σημείο 1, το σημείο 2 στοιχείο α) και τα σημεία 3, 4 και 5 πρέπει να περιλαμβάνονται στον ενωσιακό συγκεντρωτικό κατάλογο των καταλόγων εμπιστευσης σε αντικατάσταση των προηγουμένως κοινοποιηθεισών πληροφοριών που περιλαμβάνονται στον εν λόγω συγκεντρωτικό κατάλογο.

<sup>(1)</sup> ISO 3166-1: «Κωδικοί ονομάτων χωρών και υποδιαίρεσών τους — Μέρος 1: Κωδικοί χωρών».

## ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ (ΕΕ) 2015/1506 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 8ης Σεπτεμβρίου 2015

για τον καθορισμό προδιαγραφών σχετικά με τους μορφότευπους των προηγμένων ηλεκτρονικών υπογραφών και των προηγμένων σφραγίδων που πρέπει να αναγνωρίζονται από φορείς του δημόσιου τομέα σύμφωνα με τα άρθρα 27 παράγραφος 5 και 37 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για 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<sup>(1)</sup>, και ιδίως τα άρθρα 27 παράγραφος 5 και 37 παράγραφος 5,

Εκτιμώντας τα ακόλουθα:

- (1) Τα κράτη μέλη πρέπει να θέσουν σε εφαρμογή τα αναγκαία τεχνικά μέσα τα οποία θα τους επιτρέπουν να επεξεργάζονται τα ηλεκτρονικώς υπογεγραμμένα έγγραφα που απαιτούνται κατά τη χρήση διαδικτυακών υπηρεσιών που προσφέρονται από φορέα του δημόσιου τομέα ή για λογαριασμό αυτού.
- (2) Ο κανονισμός (ΕΕ) αριθ. 910/2014 υποχρεώνει τα κράτη μέλη τα οποία απαιτούν προηγμένη ηλεκτρονική υπογραφή ή σφραγίδα για τη χρήση διαδικτυακών υπηρεσιών που προσφέρονται από φορέα του δημόσιου τομέα ή για λογαριασμό αυτού, να αναγνωρίζουν τις προηγμένες ηλεκτρονικές υπογραφές και σφραγίδες, τις προηγμένες ηλεκτρονικές υπογραφές και σφραγίδες που βασίζονται σε εγκεκριμένο πιστοποιητικό και τις εγκεκριμένες ηλεκτρονικές υπογραφές και σφραγίδες με συγκεκριμένους μορφότευπους, ή εναλλακτικούς μορφότευπους που επικυρώνονται σύμφωνα με συγκεκριμένες μεθόδους αναφοράς.
- (3) Για τον καθορισμό των συγκεκριμένων μορφότευπων και των μεθόδων αναφοράς, θα πρέπει να ληφθούν υπόψη οι ισχύουσες πρακτικές, τα πρότυπα και οι νομοθετικές πράξεις της Ένωσης.
- (4) Με την εκτελεστική απόφαση 2014/148/ΕΕ<sup>(2)</sup> της Επιτροπής καθορίστηκαν ορισμένοι από τους πλέον κοινούς μορφότευπους προηγμένων ηλεκτρονικών υπογραφών που πρέπει να υποστηρίζονται τεχνικά από τα κράτη μέλη, στις περιπτώσεις στις οποίες απαιτούνται προηγμένες ηλεκτρονικές υπογραφές για διαδικτυακές διοικητικές διαδικασίες. Ο καθορισμός των μορφότευπων αναφοράς αποσκοπεί στη διευκόλυνση της διασυννοριακής επικύρωσης των ηλεκτρονικών υπογραφών και στη βελτίωση της διασυννοριακής διαλειτουργικότητας των ηλεκτρονικών διαδικασιών.
- (5) Τα πρότυπα που απαριθμούνται στο παράρτημα της παρούσας απόφασης αποτελούν τα υφιστάμενα πρότυπα για τους μορφότευπους προηγμένων ηλεκτρονικών υπογραφών. Λόγω της υπό εξέλιξη αναθεώρησης από τους οργανισμούς τυποποίησης των μακροπρόθεσμων αρχειακών μορφών των αναφερόμενων μορφότευπων, τα πρότυπα τα οποία αναλύουν λεπτομερώς τη μακροχρόνια αρχειοθέτηση εξαιρούνται από το πεδίο εφαρμογής της παρούσας απόφασης. Όταν διατεθεί νέα έκδοση των αναφερόμενων προτύπων, θα επανεξεταστούν οι αναφορές στα πρότυπα και τις ρήτρες σχετικά με τη μακροπρόθεσμη αρχειοθέτηση.
- (6) Οι προηγμένες ηλεκτρονικές υπογραφές και οι προηγμένες ηλεκτρονικές σφραγίδες είναι παρόμοιες από τεχνική άποψη. Ως εκ τούτου, τα πρότυπα για τους μορφότευπους προηγμένων ηλεκτρονικών υπογραφών θα πρέπει να ισχύουν κατ' αναλογία και για τους μορφότευπους προηγμένων ηλεκτρονικών σφραγίδων.
- (7) Όπου χρησιμοποιούνται διαφορετικοί μορφότευποι ηλεκτρονικής υπογραφής ή σφραγίδας για υπογραφή ή σφράγιση σε σχέση με εκείνους που συνήθως υποστηρίζονται τεχνικά, θα πρέπει να παρέχονται μέσα τα οποία να επιτρέπουν την επικύρωση ηλεκτρονικών υπογραφών και σφραγίδων που θα επαληθεύονται διασυννοριακά. Προκειμένου να μπορέσουν τα κράτη μέλη αποδέκτες να βασίζονται στα εργαλεία επικύρωσης άλλου κράτους μέλους, είναι αναγκαίο να παρέχονται εύκολα προσβάσιμες πληροφορίες σχετικά με τα εν λόγω εργαλεία επικύρωσης με τη συμπερίληψη των πληροφοριών στα ηλεκτρονικά έγγραφα, στις ηλεκτρονικές υπογραφές ή στους περιέκτες ηλεκτρονικών εγγράφων.

<sup>(1)</sup> ΕΕ L 257 της 28.8.2014, σ. 73.

<sup>(2)</sup> Εκτελεστική απόφαση 2014/148/ΕΕ της Επιτροπής, της 17ης Μαρτίου 2014, για την τροποποίηση της απόφασης 2011/130/ΕΕ της Επιτροπής περί καθιέρωσης ελάχιστων απαιτήσεων για τη διασυννοριακή επεξεργασία εγγράφων τα οποία έχουν υπογραφεί ηλεκτρονικά από αρμόδιες αρχές, σύμφωνα με την οδηγία 2006/123/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με τις υπηρεσίες στην εσωτερική αγορά (ΕΕ L 80 της 19.3.2014, σ. 7).

- (8) Όπου υπάρχουν διαθέσιμες δυνατότητες επικύρωσης ηλεκτρονικής υπογραφής ή σφραγίδας κατάλληλες για αυτοματοποιημένη επεξεργασία στις δημόσιες υπηρεσίες ενός κράτους μέλους, οι εν λόγω δυνατότητες επικύρωσης θα πρέπει να διατίθενται και να παρέχονται στο κράτος μέλος αποδέκτη. Ωστόσο, η παρούσα απόφαση δεν θα πρέπει να εμποδίζει την εφαρμογή των άρθρων 27 παράγραφοι 1 και 2 και 37 παράγραφοι 1 και 2 του κανονισμού (ΕΕ) αριθ. 910/2014 όταν δεν είναι δυνατή η αυτοματοποιημένη επεξεργασία των δυνατοτήτων επικύρωσης εναλλακτικών μεθόδων
- (9) Προκειμένου να προβλεφθούν παρόμοιες απαιτήσεις επικύρωσης και να αυξηθεί η εμπιστοσύνη στις δυνατότητες επικύρωσης που προβλέπονται από τα κράτη μέλη για άλλους μορφότυπους ηλεκτρονικής υπογραφής ή σφραγίδας πέραν εκείνων που τυγχάνουν κοινής υποστήριξης, οι απαιτήσεις που ορίζονται στην παρούσα απόφαση για τα εργαλεία επικύρωσης, αντλούν από τις απαιτήσεις για την επικύρωση των αναγνωρισμένων ηλεκτρονικών υπογραφών και σφραγίδων που αναφέρονται στα άρθρα 32 και 40 του κανονισμού (ΕΕ) αριθ. 910/2014.
- (10) Τα μέτρα που προβλέπονται στην παρούσα απόφαση είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 48 του κανονισμού (ΕΕ) αριθ. 910/2014,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

#### Άρθρο 1

Τα κράτη μέλη που απαιτούν προηγμένη ηλεκτρονική υπογραφή ή προηγμένη ηλεκτρονική υπογραφή η οποία βασίζεται σε αναγνωρισμένο πιστοποιητικό όπως προβλέπεται στο άρθρο 27 παράγραφοι 1 και 2 του κανονισμού (ΕΕ) αριθ. 910/2014, αναγνωρίζουν προηγμένη ηλεκτρονική υπογραφή XML, CMS ή PDF σε επίπεδο συμμόρφωσης B, T ή LT ή με χρήση συναφούς περιέκτη υπογραφής, όπου οι εν λόγω υπογραφές πληρούν τις τεχνικές προδιαγραφές που παρατίθενται στο παράρτημα.

#### Άρθρο 2

1. Τα κράτη μέλη που απαιτούν προηγμένη ηλεκτρονική υπογραφή ή προηγμένη ηλεκτρονική υπογραφή η οποία βασίζεται σε αναγνωρισμένο πιστοποιητικό όπως προβλέπεται στο άρθρο 27, παράγραφοι 1 και 2 του κανονισμού (ΕΕ) αριθ. 910/2014, αναγνωρίζουν μορφότυπους ηλεκτρονικών υπογραφών διαφορετικούς από αυτούς που αναφέρονται στο άρθρο 1 της παρούσας απόφασης, υπό την προϋπόθεση ότι το κράτος μέλος στο οποίο είναι εγκατεστημένος ο πάροχος υπηρεσιών εμπιστοσύνης που χρησιμοποιείται από τον υπογράφοντα, προσφέρει σε άλλα κράτη μέλη δυνατότητες επικύρωσης υπογραφής, όπου είναι δυνατόν, κατάλληλες για αυτοματοποιημένη επεξεργασία.

2. Οι δυνατότητες επικύρωσης υπογραφής:

α) επιτρέπουν σε άλλα κράτη μέλη την επικύρωση της παραλαμβανόμενης ηλεκτρονικής υπογραφής με διαδικτυακά μέσα, δωρεάν και κατά τρόπο κατανοητό για τους μη φυσικούς ομιλητές·

β) αναφέρονται στο υπογεγραμμένο έγγραφο, στην ηλεκτρονική υπογραφή ή στον περιέκτη ηλεκτρονικών εγγράφων· και

γ) επιβεβαιώνουν την εγκυρότητα μιας προηγμένης ηλεκτρονικής υπογραφής, υπό την προϋπόθεση ότι:

1) το πιστοποιητικό που υποστηρίζει την προηγμένη ηλεκτρονική υπογραφή ήταν έγκυρο κατά τη στιγμή της υπογραφής, και, στην περίπτωση που η προηγμένη ηλεκτρονική υπογραφή υποστηρίζεται από αναγνωρισμένο πιστοποιητικό, το αναγνωρισμένο πιστοποιητικό το οποίο υποστηρίζει την προηγμένη ηλεκτρονική υπογραφή ήταν, κατά τη στιγμή της υπογραφής, αναγνωρισμένο πιστοποιητικό ηλεκτρονικής υπογραφής σύμφωνο με τις διατάξεις του παραρτήματος I του κανονισμού (ΕΕ) αριθ. 910/2014 και είχε εκδοθεί από αναγνωρισμένο πάροχο υπηρεσιών εμπιστοσύνης·

2) τα στοιχεία επικύρωσης της υπογραφής αντιστοιχούν στα δεδομένα που παρέχονται στο βασικό μέρος·

3) το μοναδικό σύνολο δεδομένων που αντιπροσωπεύουν τον υπογράφοντα παρέχεται ορθώς στο βασικό μέρος·

4) η χρήση οποιουδήποτε ψευδώνυμου δηλώνεται εμφανώς στο βασικό μέρος, εάν κατά τη στιγμή της υπογραφής χρησιμοποιήθηκε ψευδώνυμο·



- 5) όταν η προηγμένη ηλεκτρονική υπογραφή δημιουργείται από αναγνωρισμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής, η χρήση οποιασδήποτε τέτοιας διάταξης δηλώνεται εμφανώς στο βασικό μέρος·
- 6) η ακεραιότητα των υπογεγραμμένων δεδομένων δεν έχει παραβιαστεί·
- 7) κατά τη στιγμή της υπογραφής πληρούνταν οι απαιτήσεις που προβλέπονται στο άρθρο 26 του κανονισμού (ΕΕ) αριθ. 910/2014·
- 8) το σύστημα που χρησιμοποιείται για την επικύρωση της προηγμένης ηλεκτρονικής υπογραφής παρέχει στο βασικό μέρος το ορθό αποτέλεσμα της διαδικασίας επικύρωσης και του επιτρέπει να εντοπίζει τυχόν ζητήματα ασφαλείας.

### Άρθρο 3

Τα κράτη μέλη που απαιτούν προηγμένη ηλεκτρονική σφραγίδα ή προηγμένη ηλεκτρονική σφραγίδα με βάση αναγνωρισμένο πιστοποιητικό όπως προβλέπεται στο άρθρο 37 παράγραφοι 1 και 2 του κανονισμού (ΕΕ) αριθ. 910/2014, αναγνωρίζουν προηγμένη ηλεκτρονική σφραγίδα XML, CMS ή PDF σε επίπεδο συμμόρφωσης B, T ή LT ή με χρήση συναφούς περιέκτη σφραγίδας εφόσον πληρούνται οι τεχνικές προδιαγραφές που παρατίθενται στο παράρτημα.

### Άρθρο 4

1. Τα κράτη μέλη που απαιτούν προηγμένη ηλεκτρονική σφραγίδα ή προηγμένη ηλεκτρονική σφραγίδα με βάση αναγνωρισμένο πιστοποιητικό όπως προβλέπεται στο άρθρο 37 παράγραφοι 1 και 2 του κανονισμού (ΕΕ) αριθ. 910/2014, αναγνωρίζουν άλλους μορφότυπους ηλεκτρονικών σφραγίδων εκτός από αυτούς που αναφέρονται στο άρθρο 3 της παρούσας απόφασης, υπό την προϋπόθεση ότι το κράτος μέλος στο οποίο είναι εγκατεστημένος ο πάροχος υπηρεσιών εμπιστοσύνης που χρησιμοποιείται από τον δημιουργό της σφραγίδας, προσφέρει σε άλλα κράτη μέλη δυνατότητες επικύρωσης σφραγίδας, κατάλληλες, όπου είναι δυνατόν, για αυτοματοποιημένη επεξεργασία.

2. Οι δυνατότητες επικύρωσης σφραγίδας:

- a) επιτρέπουν σε άλλα κράτη μέλη την επικύρωση των παραλαμβανόμενων ηλεκτρονικών σφραγίδων διαδικτυακά, δωρεάν και κατά τρόπο κατανοητό για τους μη φυσικούς ομιλητές·
- β) αναφέρονται στο σφραγισμένο έγγραφο, στην ηλεκτρονική σφραγίδα ή στον περιέκτη ηλεκτρονικών εγγράφων·
- γ) επιβεβαιώνουν την εγκυρότητα μιας προηγμένης ηλεκτρονικής σφραγίδας υπό την προϋπόθεση ότι:
  - 1) το πιστοποιητικό που υποστηρίζει την προηγμένη ηλεκτρονική σφραγίδα ήταν έγκυρο κατά τη στιγμή της σφράγισης, και, στην περίπτωση που η προηγμένη ηλεκτρονική σφραγίδα υποστηρίζεται από αναγνωρισμένο πιστοποιητικό, το αναγνωρισμένο πιστοποιητικό που υποστηρίζει την προηγμένη ηλεκτρονική σφραγίδα ήταν, κατά τη στιγμή της σφράγισης, αναγνωρισμένο πιστοποιητικό ηλεκτρονικής σφραγίδας σύμφωνα με τις διατάξεις του παραρτήματος III του κανονισμού (ΕΕ) αριθ. 910/2014 και έχει εκδοθεί από αναγνωρισμένο πάροχο υπηρεσιών εμπιστοσύνης·
  - 2) τα δεδομένα επικύρωσης σφραγίδας αντιστοιχούν στα δεδομένα που παρέχονται στο βασικό μέρος·
  - 3) το μοναδικό σύνολο δεδομένων που αντιπροσωπεύουν τον δημιουργό σφραγίδας παρέχεται ορθώς στο βασικό μέρος·
  - 4) η χρήση οποιοδήποτε ψευδώνυμου δηλώνεται εμφανώς στο βασικό μέρος, εάν κατά τη στιγμή της σφράγισης χρησιμοποιήθηκε ψευδώνυμο·
  - 5) όταν η προηγμένη ηλεκτρονική σφραγίδα δημιουργείται από αναγνωρισμένη διάταξη δημιουργίας ηλεκτρονικής σφραγίδας, η χρήση οποιασδήποτε τέτοιας διάταξης δηλώνεται εμφανώς στο βασικό μέρος·
  - 6) η ακεραιότητα των σφραγισμένων δεδομένων δεν έχει παραβιαστεί·
  - 7) κατά τη στιγμή της σφράγισης πληρούνταν οι απαιτήσεις που προβλέπονται στο άρθρο 36 του κανονισμού (ΕΕ) αριθ. 910/2014·
  - 8) το σύστημα που χρησιμοποιείται για την επικύρωση της προηγμένης ηλεκτρονικής σφραγίδας παρέχει στο βασικό μέρος το ορθό αποτέλεσμα της διαδικασίας επικύρωσης και του επιτρέπει να εντοπίζει τυχόν ζητήματα ασφαλείας.

*Άρθρο 5*

Η παρούσα απόφαση αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Η παρούσα απόφαση είναι δεσμευτική 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

**Κατάλογος τεχνικών προδιαγραφών για προηγμένες ηλεκτρονικές υπογραφές XML, CMS ή PDF και τον συναφή περιέκτη υπογραφής**

Οι προηγμένες ηλεκτρονικές υπογραφές που αναφέρονται στο άρθρο 1 της απόφασης πρέπει να πληρούν μία από τις ακόλουθες τεχνικές προδιαγραφές του ETSI εξαιρουμένης της ρήτρας 9:

Βασικό προφίλ XAdES	ETSI TS 103171 v.2.1.1 <sup>(1)</sup>
Βασικό προφίλ CAdES	ETSI TS 103173 v.2.1.1 <sup>(2)</sup>
Βασικό προφίλ PAdES	ETSI TS 103172 v.2.2.2 <sup>(3)</sup>

<sup>(1)</sup> [http://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103171/02.01.01\\_60/ts\\_103171v020101p.pdf](http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf)  
<sup>(2)</sup> [http://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103173/02.02.01\\_60/ts\\_103173v020201p.pdf](http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf)  
<sup>(3)</sup> [http://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103172/02.02.02\\_60/ts\\_103172v020202p.pdf](http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf)

Ο συναφής περιέκτης υπογραφής που αναφέρεται στο άρθρο 1 της απόφασης πρέπει να πληροί τις ακόλουθες τεχνικές προδιαγραφές του ETSI:

Βασικό προφίλ συναφούς περιέκτη υπογραφής	ETSI TS 103174 v.2.2.1 <sup>(1)</sup>
---	---------------------------------------

<sup>(1)</sup> [http://www.etsi.org/deliver/etsi\\_ts/103100\\_103199/103174/02.02.01\\_60/ts\\_103174v020201p.pdf](http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf)

**Κατάλογος τεχνικών προδιαγραφών για προηγμένες ηλεκτρονικές σφραγίδες XML, CMS ή PDF και τον συναφή περιέκτη σφραγίδας**

Οι προηγμένες ηλεκτρονικές σφραγίδες που αναφέρονται στο άρθρο 3 της απόφασης πρέπει να πληρούν μία από τις ακόλουθες τεχνικές προδιαγραφές του ETSI εξαιρουμένης της ρήτρας 9:

Βασικό προφίλ XAdES	ETSI TS 103171 v.2.1.1
Βασικό προφίλ CAdES	ETSI TS 103173 v.2.2.1
Βασικό προφίλ PAdES	ETSI TS 103172 v.2.2.2

Ο συναφής περιέκτης σφραγίδας που αναφέρεται στο άρθρο 3 της απόφασης πρέπει να πληροί τις ακόλουθες τεχνικές προδιαγραφές του ETSI:

Βασικό προφίλ συναφούς περιέκτη σφραγίδας	ETSI TS 103174 v.2.2.1.
---	-------------------------









ISSN 1977-0669 (ηλεκτρονική έκδοση)  
ISSN 1725-2547 (έντυπη έκδοση)



**Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης**  
2985 Λουξεμβούργο  
ΛΟΥΞΕΜΒΟΥΡΓΟ

**EL**