ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

ΤΕΥΧΟΣ ΔΗΜΟΣΙΑΣ ΔΙΑΒΟΥΛΕΥΣΗΣ

Θέμα: Εισήγηση της ΕΕΤΤ για την έκδοση Υ.Α. σύμφωνα με το άρθρο 107 παρ. 33 Ν. 4727/2020 (ΦΕΚ Α' 184/23.09.2020) με αντικείμενο τη ρύθμιση των υποχρεώσεων των παρόχων υπηρεσιών εμπιστοσύνης, εγκεκριμένων και μη, της διαδικασίας χορήγησης έγκρισης και έναρξης παροχής νέων υπηρεσιών εμπιστοσύνης και λοιπών συναφών θεμάτων

Μαρούσι, Ιούλιος 2021

Το παρόν Τεύχος Δημόσιας Διαβούλευσης έχει ετοιμαστεί από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και έχει ως θεματικό αντικείμενο την ρύθμιση των υποχρεώσεων των παρόχων υπηρεσιών εμπιστοσύνης, εγκεκριμένων και μη, της διαδικασίας χορήγησης έγκρισης και έναρξης παροχής νέων υπηρεσιών εμπιστοσύνης και λοιπών συναφών θεμάτων, με σκοπό την υποβολή εισήγησης της ΕΕΤΤ προς τον Υπουργό Ψηφιακής Διακυβέρνησης, σύμφωνα με τα προβλεπόμενα στο άρθρο 107 παρ. 33 Ν. 4727/2020 (ΦΕΚ Α' 184/23.09.2020)

Η ΕΕΤΤ προσκαλεί τους ενδιαφερόμενους φορείς να υποβάλουν τα σχόλια και τις απόψεις τους σχετικά με την πρότασή της προς τον Υπουργό Ψηφιακής Διακυβέρνησης για τον ορισμό υποχρεώσεων των παρόχων υπηρεσιών εμπιστοσύνης, εγκεκριμένων και μη, της διαδικασίας χορήγησης έγκρισης και έναρξης παροχής νέων υπηρεσιών εμπιστοσύνης και λοιπών συναφών θεμάτων, όπως διαμορφώνεται στο παρόν Τεύχος Δημόσιας Διαβούλευσης, προκειμένου να υποβληθεί εν συνεχεία η εισήγηση της ΕΕΤΤ για την έκδοση της προβλεπόμενης στον ως άνω νόμο υπουργικής απόφασης.

Αν υπάρχουν απόψεις ή σχόλια που δεν καλύπτονται από το παρόν κείμενο Δημόσιας Διαβούλευσης, παρακαλούμε να τα συμπεριλάβετε στις απαντήσεις σας.

Οι απαντήσεις πρέπει να υποβληθούν επωνύμως, στην Ελληνική γλώσσα, σε έντυπη ή/και σε ηλεκτρονική μορφή στην ηλεκτρονική διεύθυνση eidas@eett.gr όχι αργότερα από την **17η Σεπτεμβρίου 2021** και ώρα 15:00. Τυχόν ανώνυμες απαντήσεις δεν θα ληφθούν υπόψη.

Η ΕΕΤΤ διατηρεί το δικαίωμα δημοσίευσης των απαντήσεων στη ΔΔ, καθώς και των ονομάτων των μερών που θα συμμετάσχουν σε αυτήν. Σε περίπτωση που κάποιο ενδιαφερόμενο μέρος θεωρεί την απάντησή του εν μέρει ή συνολικά εμπιστευτική, θα πρέπει να έχει επισημάνει σαφώς τα σημεία της απάντησής του που θεωρεί εμπιστευτικά, ή ότι θεωρεί όλη την απάντησή του εμπιστευτική. Σε κάθε περίπτωση η ΕΕΤΤ θα έχει δικαίωμα να δημοσιεύσει τα ονόματα των συμμετεχόντων στη ΔΔ.

Οι απαντήσεις πρέπει να υποβάλλονται ηλεκτρονικά στην ακόλουθη διεύθυνση ηλεκτρονικού ταχυδρομείου: E-mail : eidas@eett.gr

Κατά τη διάρκεια της Δημόσιας Διαβούλευσης είναι δυνατό να παρέχονται από την ΕΕΤΤ διευκρινιστικές απαντήσεις σε ερωτήσεις των ενδιαφερομένων, οι οποίες πρέπει να υποβάλλονται επώνυμα, μόνο μέσω του ηλεκτρονικού ταχυδρομείου στη διεύθυνση: eidas@eett.gr.

ΠΡΟΤΕΙΝΟΜΕΝΟ ΠΕΡΙΕΧΟΜΕΝΟ

Υπουργικής Απόφασης άρθρου 107, σημείου 33 του ν.4727/2020

Μέρος Α: Γενικές Διατάξεις

Άρθρο 1

Σκοπός και πεδίο εφαρμογής

Σκοπός της παρούσας είναι ο καθορισμός των υποχρεώσεων των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών εμπιστοσύνης, η διαδικασία χορήγησης έγκρισης, οι λεπτομέρειες αναφορικά με την έναρξη νέων υπηρεσιών εμπιστοσύνης, καθώς και κάθε σχετικό θέμα για την εφαρμογή του άρθρου 52 του ν.4727/2020.

Άρθρο 2

Ορισμοί και Ακρωνύμια

1. Για την εφαρμογή της παρούσας ισχύουν οι ακόλουθοι ορισμοί:

Κανονισμός eIDAS: 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.

Κατάλογος Υπηρεσιών Εμπιστοσύνης (Trust Service List - TSL): Ο κατάλογος υπηρεσιών εμπιστοσύνης περιλαμβάνει πληροφορίες σχετικά με τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης εγκατεστημένους στην Ελλάδα, και τις εγκεκριμένες υπηρεσίες εμπιστοσύνης που αυτοί παρέχουν. Τον Κατάλογο Υπηρεσιών Εμπιστοσύνης καταρτίζει, τηρεί και δημοσιεύει η ΕΕΤΤ.

Σχέδιο Τερματισμού Εργασιών (Termination Plan): Πρόκειται για το αναλυτικό σχέδιο όλων των ενεργειών στις οποίες οφείλει να προβεί ο κάθε εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης προκείμενου να τερματίσει την παροχή κάποιας εγκεκριμένης υπηρεσίας εμπιστοσύνης ή και της λειτουργίας του εν γένει. Το εν λόγω σχέδιο οφείλει να καλύπτει και κάθε μη προγραμματισμένη, ακούσια διακοπή των δραστηριοτήτων, όπως σε περίπτωση πτώχευσης.

2. Λοιπές λέξεις ή φράσεις που χρησιμοποιούνται στον παρόντα Κανονισμό έχουν την έννοια που τους αποδίδει ο Κανονισμός (ΕΕ) 910/2014 (eIDAS).

3. Ακρωνύμια

ΠΥΕ: Πάροχος Υπηρεσιών Εμπιστοσύνης (Trust Service Provider, TSP)

ΕΑΣ : Έκθεση Αξιολόγησης Συμμόρφωσης (Conformity Assessment Report, CAR)

ΟΑΣ : Οργανισμός Αξιολόγησης Συμμόρφωσης (Conformity Assessment Body, CAB)

CP : Certificate Practice

CPS : Certificate Practice Statement

CRL : Λίστα Ανακληθέντων Πιστοποιητικών (Certificate Revocation List)

ENISA : Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών

OCSP : Ηλεκτρονικό Πρωτόκολλο Κατάστασης Πιστοποιητικού (Online Certificate Status Protocol)

Root CA : Αρχή Πιστοποίησης Ρίζας

Sub CA : Υποκείμενη Αρχή Πιστοποίησης

Μέρος Β': Έναρξη Υπηρεσιών Εμπιστοσύνης

Άρθρο 3

Τήρηση Αρχείου των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών εμπιστοσύνης

1. Η ΕΕΤΤ τηρεί ηλεκτρονικό αρχείο των εγκατεστημένων στην Ελλάδα ΠΥΕ, εγκεκριμένων και μη, σε ηλεκτρονική μορφή.
2. Στο αρχείο της παρ. 1 τηρούνται τα ακόλουθα στοιχεία:

α. ονοματεπώνυμο/επωνυμία, διεύθυνση/έδρα, τηλέφωνο, φαξ, διεύθυνση ηλεκτρονικού ταχυδρομείου, ιστοσελίδα του Παρόχου,

β. νομική μορφή, νόμιμοι εκπρόσωποι και τυχόν αντίκλητος του Παρόχου,

γ. αριθμός Φορολογικού Μητρώου (ΑΦΜ) και αρμόδια Διεύθυνση Οικονομικών Υπηρεσιών (ΔΟΥ),

δ. αριθμός Γενικού Εμπορικού Μητρώου (Γ.Ε.ΜΗ.),

ε. πλήρη στοιχεία επικοινωνίας των υπευθύνων επικοινωνίας με την ΕΕΤΤ,

στ. πλήρη στοιχεία επικοινωνίας με το κοινό προκειμένου να δημοσιευθούν στην ιστοσελίδα της ΕΕΤΤ,

ζ. παρεχόμενες υπηρεσίες (άρθρο 3, σημ. 16 και 17 του Κανονισμού eIDAS).

Άρθρο 4

Παροχή μη εγκεκριμένων υπηρεσιών εμπιστοσύνης

1. Για την παροχή μη εγκεκριμένων υπηρεσιών εμπιστοσύνης δεν απαιτείται προηγούμενη έγκριση ή άδεια.
2. Οι μη εγκεκριμένοι ΠΥΕ, που παρέχουν υπηρεσίες στο ευρύ κοινό, υποχρεούνται να εγγραφούν στο Αρχείο της ΕΕΤΤ. Για την εγγραφή τους, υποβάλλουν αίτηση/ υπεύθυνη δήλωση με τα στοιχεία που αναφέρονται στο άρθρο 3 παρ. 2 και τέλος καταχώρισης, ύψους 200€ (διακοσίων ευρώ). Η διαδικασία υποβολής της αίτησης καθορίζεται από την ΕΕΤΤ.
3. Η ΕΕΤΤ δύναται να ζητήσει κατά περίπτωση επιπλέον στοιχεία και κάθε αναγκαία διευκρίνιση για την εξέταση του αιτήματος.
4. Σε περίπτωση που η ΕΕΤΤ γίνει αποδέκτης πληροφοριών, σύμφωνα με τις οποίες κάποιος μη εγκεκριμένος ΠΥΕ ή οι υπηρεσίες εμπιστοσύνης που παρέχει ενδέχεται να μην πληρούν τις απαιτήσεις του Κανονισμού eIDAS, δύναται να καλεί τον ΠΥΕ να υποβάλει τις απόψεις του, καθώς και στοιχεία που αποδεικνύουν τη συμμόρφωσή του με τον Κανονισμό eIDAS.

Άρθρο 5

Έναρξη εγκεκριμένων υπηρεσιών εμπιστοσύνης

1. Έγκριση για την παροχή εγκεκριμένων υπηρεσιών εμπιστοσύνης χορηγείται από την ΕΕΤΤ, κατόπιν σχετικού αιτήματος των ενδιαφερομένων. Μη εγκεκριμένοι ΠΥΕ, που είναι ήδη καταχωρισμένοι στο αρχείο της ΕΕΤΤ και επιθυμούν να παρέχουν εγκεκριμένες υπηρεσίες εμπιστοσύνης, κοινοποιούν την πρόθεσή τους στην ΕΕΤΤ, υποβάλλοντας αίτηση σύμφωνα με τις διατάξεις του παρόντος άρθρου. Αντίστοιχη κοινοποίηση υποβάλλουν εγκεκριμένοι ΠΥΕ που επιθυμούν να παρέχουν εγκεκριμένη υπηρεσία εμπιστοσύνης για την οποία δεν έχουν λάβει έγκριση από την ΕΕΤΤ, οι οποίοι εξαιρούνται από την υποχρέωση υποβολής των εγγράφων που αναφέρονται στα σημεία (β), (γ), (δ), (ε), (στ), (ζ) και (ιβ) της παρ. 4 κατωτέρω αλλά και εγκεκριμένοι ΠΥΕ που επιθυμούν την ενεργοποίηση νέας αρχής πιστοποίησης για έκδοση εγκεκριμένων πιστοποιητικών για υπηρεσία εμπιστοσύνης για την οποία έχουν λάβει έγκριση από την ΕΕΤΤ, οι οποίοι έχουν υποχρέωση υποβολής μόνο των εγγράφων που αναφέρονται στα σημεία (η) και (θ) της παρ. 4 κατωτέρω. Για την εξέταση αιτήματος μη εγκεκριμένου ΠΥΕ, επιβάλλεται τέλος ύψους 1000€ (χιλίων ευρώ), το οποίο καταβάλλεται με την υποβολή της αίτησης.

2. Με την υποβολή του αιτήματος εκκινεί η Διαδικασία Έναρξης Παροχής Εγκεκριμένων Υπηρεσιών (διαδικασία «έναρξης εγκεκριμένης υπηρεσίας εμπιστοσύνης»), κατά την οποία η ΕΕΤΤ εξετάζει εάν ο αιτών και οι παρεχόμενες από αυτόν υπηρεσίες εμπιστοσύνης συμμορφώνονται με τις απαιτήσεις του Κανονισμού eIDAS, του ν.4727/2020, της παρούσας απόφασης και τυχόν άλλων διατάξεων που αφορούν εγκεκριμένα πιστοποιητικά. Στον εν λόγω έλεγχο υποβάλλεται χωριστά κάθε υπηρεσία εμπιστοσύνης (από τις προβλεπόμενες στον Κανονισμό eIDAS) που επιθυμεί να παρέχει ο αιτών και δεν έχει ακόμα εγκριθεί.

3. Ο αιτών, εφόσον δεν είναι καταχωρισμένος στο ηλεκτρονικό αρχείο της ΕΕΤΤ ως εγκεκριμένος πάροχος, υποβάλλει αίτηση εγγραφής, χωρίς να απαιτείται καταβολή του τέλους καταχώρισης. Η διαδικασία υποβολής της αίτησης καθορίζεται από την ΕΕΤΤ.

4. Ο αιτών υποβάλλει ηλεκτρονικά στην ΕΕΤΤ τη σχετική αίτηση/ υπεύθυνη δήλωση (Παράρτημα 2 της παρούσας απόφασης) συνοδευόμενη από τα παρακάτω έγγραφα, κατά περίπτωση:

   α) Έκθεση Αξιολόγησης της Συμμόρφωσης (ΕΑΣ) εκδοθείσα από Οργανισμό Αξιολόγησης της Συμμόρφωσης (ΟΑΣ) σύμφωνα με το άρθρο 13 της παρούσας Απόφασης.

   β) Πιστοποιητικό εγγραφής στο Γενικό Εμπορικό Μητρώο (Γ.Ε.ΜΗ.).

   γ) Πιστοποιητικό/ βεβαίωση του οικείου επαγγελματικού ή εμπορικού μητρώου για την εγγραφή του σε αυτό. Εφόσον πρόκειται για νομικό πρόσωπο, πιστοποιητικό/ βεβαίωση εμπορικού επιμελητηρίου ή άλλης αντίστοιχης αρμόδιας δημόσιας υπηρεσίας, από το οποίο να προκύπτει, κατά περίπτωση, η νόμιμη σύσταση του αιτούντος, όλες οι τροποποιήσεις των καταστατικών, το/τα πρόσωπο/α που δεσμεύει/ουν νόμιμα την εταιρεία κατά την ημερομηνία υποβολής της αίτησης (νόμιμος εκπρόσωπος, δικαίωμα υπογραφής κ.λπ.), τυχόν τρίτοι στους οποίους έχει χορηγηθεί εξουσία εκπροσώπησης, καθώς και η θητεία του ή/και των μελών του οργάνου διοίκησης/ νόμιμου εκπροσώπου.

   δ) Βεβαιώσεις ασφαλιστικής και φορολογικής ενημερότητας.

   ε) Ενιαίο Πιστοποιητικό Δικαστικής Φερεγγυότητας από το αρμόδιο Πρωτοδικείο, από το οποίο προκύπτει ότι δεν τελούν υπό πτώχευση, πτωχευτικό συμβιβασμό ή υπό αναγκαστική διαχείριση ή δικαστική εκκαθάριση ή ότι δεν έχουν υπαχθεί σε διαδικασία εξυγίανσης.

στ) Εκτύπωση της καρτέλας «Στοιχεία Μητρώου/Επιχείρησης» από την ηλεκτρονική πλατφόρμα της Ανεξάρτητης Αρχής Δημοσίων Εσόδων, όπως αυτά εμφανίζονται στο Taxisnet, από την οποία να προκύπτει η μη αναστολή της επιχειρηματικής δραστηριότητάς τους.

ζ) Τους ισολογισμούς των δύο (2) τελευταίων ετών, που έχουν ολοκληρωθεί, εφόσον δημοσιεύονται, ή υπεύθυνη δήλωση του Ν. 1599/1986 του συνολικού ύψους του ετήσιου κύκλου εργασιών τα δύο (2) τελευταία χρόνια, σε περίπτωση που δεν υπάρχει υποχρέωση δημοσίευσης. Εφόσον ο αιτών δραστηριοποιείται για μικρότερο χρονικό διάστημα, υποβάλλει αποσπάσματα οικονομικών καταστάσεων ή δήλωση για το εν λόγω χρονικό διάστημα.

η) Δηλωτικά έγγραφα, τα οποία περιγράφουν την Πολιτική Υπηρεσίας Εμπιστοσύνης (Trust Service Policy) και τη Δήλωση Πρακτικής του Παρόχου (Trust Service Practice Statement) για τις υπό έγκριση υπηρεσίες.

θ) Πιστοποιητικά των Αρχών Πιστοποίησης που θα χρησιμοποιηθούν για την παροχή της υπηρεσίας και δείγματα (Test samples) των πιστοποιητικών ή άλλων στοιχείων που θα εκδοθούν ή θα δημιουργηθούν στο πλαίσιο κάθε υπό έγκριση υπηρεσίας.

ι) Αναφορά αποτίμησης κινδύνου σύμφωνα με τις απαιτήσεις του Άρθρου 19, παρ. 1 του Κανονισμού eIDAS (Παράρτημα 1 της παρούσας Απόφασης).

ια) Σχέδιο Ειδοποίησης του τελικού χρήστη, σε περίπτωση συμβάντος ασφαλείας, σύμφωνα με τις απαιτήσεις του Άρθρου 19, παρ. 2 του Κανονισμού eIDAS.

ιβ) Σχέδιο Τερματισμού λειτουργίας του εν λόγω Παρόχου (άρθρο 11 της παρούσας απόφασης), σύμφωνα με τα άρθρα 17, παρ. 4, στ. (θ) και 24, παρ. 2, στ. (θ) του Κανονισμού eIDAS.

ιγ) Αντίγραφο της τυποποιημένης Σύμβασης με τους τελικούς χρήστες που περιλαμβάνει τους Όρους Χρήσης της υπηρεσίας.

5. Η ΕΕΤΤ υποχρεούται εντός πέντε (5) εργάσιμων ημερών από την κατάθεση της αίτησης, να επιβεβαιώσει ότι η αίτηση περιλαμβάνει το σύνολο των παραπάνω εγγράφων ή ειδικώς να προσδιορίσει ποιο έγγραφο υπολείπεται και να το ζητήσει εγγράφως από τον αιτούντα την έγκριση. Ο αιτών οφείλει να προσκομίσει κάθε έγγραφο που τυχόν ζητηθεί εντός χρονικής προθεσμίας που θα τεθεί από την κοινοποίηση της σχετικής επιστολής της ΕΕΤΤ. Η χρονική προθεσμία θα ορίζεται από την ΕΕΤΤ κατά περίπτωση και δεν μπορεί να είναι μικρότερη από πέντε (5) εργάσιμες ημέρες και μεγαλύτερη από εικοσιπέντε (25) εργάσιμες ημέρες. Σε περίπτωση μη έγκαιρης υποβολής των απαιτούμενων στοιχείων από τον αιτούντα, η αίτηση απορρίπτεται.

6. Η ΕΕΤΤ δύναται να ζητήσει κατά περίπτωση επιπλέον στοιχεία και κάθε αναγκαία διευκρίνιση κατά τον έλεγχο της συμμόρφωσης του αιτούντος.

7. Η ΕΕΤΤ εξετάζει την ΕΑΣ και τα συνοδευτικά της έγγραφα προκειμένου να διαπιστώσει τη συμμόρφωση με τις σχετικές απαιτήσεις και με αιτιολογημένη απόφασή της εγκρίνει, ορίζοντας σαφώς το χρόνο έναρξης παροχής της εγκεκριμένης υπηρεσίας, ή απορρίπτει το αίτημα του αιτούντα, εντός τριών (3) μηνών από την κοινοποίησή του. Εάν η εξέταση της συμμόρφωσης του αιτούντα δεν ολοκληρωθεί εντός της ανωτέρω προθεσμίας, η ΕΕΤΤ ενημερώνει σχετικά τον αιτούντα, εξηγώντας τους λόγους της καθυστέρησης και ορίζοντας νέα προθεσμία εντός της οποίας θα ολοκληρωθεί η διαδικασία. Σε περίπτωση έγκρισης, η ΕΕΤΤ ενημερώνει κατάλληλα το αρχείο των παρόχων υπηρεσιών εμπιστοσύνης που τηρεί, εφόσον απαιτείται, καθώς και τον Κατάλογο Υπηρεσιών Εμπιστοσύνης.

8. Η αίτηση, απορρίπτεται στις εξής, περιοριστικά αναφερόμενες, περιπτώσεις:

α) Μη πληρότητας του φακέλου της υποβληθείσας αίτησης ή/και τυχόν αδυναμίας παροχής περαιτέρω διευκρινίσεων που ζητήθηκαν από την ΕΕΤΤ σύμφωνα με τις παραγράφους 5 και 6 ανωτέρω,

β) Μη επαρκούς τεκμηρίωσης της πλήρωσης ενός ή περισσοτέρων εκ των ανωτέρω σημείων (α) – (ιγ) της παραγράφου 4, βάσει των προσκομισθέντων εγγράφων, ή

γ) Μη πλήρωσης των απαιτήσεων που επιβάλλονται με βάση τον Κανονισμό eIDAS, το ν.4727/2020 και την παρούσα απόφαση.

9. Ο αιτών μπορεί να αρχίσει να παρέχει τις εγκεκριμένες υπηρεσίες εμπιστοσύνης μόνον μετά την ημερομηνία έναρξης της υπηρεσίας, όπως έχει καταχωριστεί στον Κατάλογο Υπηρεσιών Εμπιστοσύνης που τηρεί η ΕΕΤΤ.

10. Τα έγγραφα υπ' αριθμόν (η), (ια) και (ιγ) της παραγράφου 4 ανωτέρω πρέπει να είναι διαθέσιμα και στην Αγγλική γλώσσα, ώστε να διευκολυνθεί η συνεργασία μεταξύ των Μελών της Ένωσης. Τα έγγραφα (α), (η), (ιβ) και (ιγ) της ίδιας παραγράφου γίνονται δεκτά και στην Αγγλική γλώσσα.

Με σχόλια [SP1]:

Μέρος Γ': Υποχρεώσεις Παρόχων Υπηρεσιών Εμπιστοσύνης (εγκεκριμένων και μη)

Άρθρο 6

Απαιτήσεις ασφάλειας για τους παρόχους υπηρεσιών εμπιστοσύνης

1. Οι ΠΥΕ, εγκεκριμένοι και μη, λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα διαχείρισης των κινδύνων για την ασφάλεια των υπηρεσιών εμπιστοσύνης που παρέχουν. Τα ανωτέρω πρέπει να περιγράφονται στην αναφορά εκτίμησης κινδύνων και μέτρων αντιμετώπισης των περιστατικών ασφάλειας, που υποβάλλεται, ανάλογα με την περίπτωση, σύμφωνα με τα αναφερόμενα στο άρθρο 5, παρ. 4, σημ. (ι).

2. Οι ΠΥΕ, εγκεκριμένοι και μη, ενημερώνουν, χωρίς αδικαιολόγητη καθυστέρηση και, σε κάθε περίπτωση, εντός 24 ωρών αφότου έλαβαν γνώση σχετικά, την ΕΕΤΤ και, κατά περίπτωση, άλλους σχετικούς φορείς, για οποιαδήποτε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας που έχει σημαντικό αντίκτυπο στην παρεχόμενη υπηρεσία εμπιστοσύνης ή στα σχετικά δεδομένα προσωπικού χαρακτήρα (Κανονισμός eIDAS, άρθρο 19, παρ. 2). Σημαντικός αντίκτυπος θεωρείται ότι υπάρχει όταν λάβει χώρα συμβάν με επίπεδο επίδρασης 3 ή μεγαλύτερο, σύμφωνα με τα οριζόμενα στο άρθρο 7. Η υποχρέωση αναφοράς αφορά σε όλες τις υπηρεσίες εμπιστοσύνης, εγκεκριμένες και μη. 3. Οι ΠΥΕ, εγκεκριμένοι και μη, ενημερώνουν το φυσικό ή νομικό πρόσωπο στο οποίο παρασχέθηκε η υπηρεσία εμπιστοσύνης, το οποίο επλήγη από το περιστατικό ασφαλείας, χωρίς αδικαιολόγητη καθυστέρηση.

4. Οι ΠΥΕ, εγκεκριμένοι και μη, ενημερώνουν το κοινό, χωρίς αδικαιολόγητη καθυστέρηση για συμβάντα με επίπεδο επίδρασης τρία (3) ή μεγαλύτερο.

Άρθρο 7

Κατηγορίες συμβάντων ασφαλείας και διαδικασία αναφοράς στην ΕΕΤΤ

1. Τα συμβάντα κατατάσσονται σε πέντε επίπεδα επίδρασης:

- Επίπεδο 1. Χωρίς επιπτώσεις

- Επίπεδο 2. Ασήμαντες επιπτώσεις: Επηρεάστηκαν τα περιουσιακά στοιχεία του παρόχου αλλά δεν επηρεάστηκαν οι βασικές υπηρεσίες
- Επίπεδο 3. Σημαντικός αντίκτυπος: επηρεάζεται μέρος των πελατών / υπηρεσιών
- Επίπεδο 4. Σοβαρός αντίκτυπος: επηρεάζεται μεγάλο μέρος των πελατών / υπηρεσιών
- Επίπεδο 5. Καταστροφικές επιπτώσεις: ολόκληρη η οργάνωση, όλες οι υπηρεσίες, όλα τα πιστοποιητικά επηρεάζονται.

2. Ενδεικτικά, συμβάντα επιπέδου τρία (3) και άνω που πρέπει να αναφέρονται από τους ΠΥΕ θεωρούνται τα εξής:

α) Αποθήκευση ιδιωτικού κλειδιού:

i. Μη εξουσιοδοτημένη πρόσβαση στα ιδιωτικά κλειδιά της Root CA. ii. Μη εξουσιοδοτημένη πρόσβαση στα ιδιωτικά κλειδιά Sub CA.

iii. Μη εξουσιοδοτημένη πρόσβαση στα ιδιωτικά κλειδιά που χρησιμοποιούνται για την υπογραφή πιστοποιητικών, της CRL, των απαντήσεων μέσω OCSP.

iv. Μη εξουσιοδοτημένη πρόσβαση στα ιδιωτικά κλειδιά για τη λειτουργία της εγκεκριμένης υπηρεσίας εμπιστοσύνης.

v. Μη εξουσιοδοτημένη πρόσβαση στα ιδιωτικά κλειδιά των τελικών χρηστών λόγω ακατάλληλων μέτρων ασφαλείας του παρόχου.

vi. Μη εξουσιοδοτημένο αίτημα χρήσης κλειδιού που ανήκει σε τρίτο μέρος για την έκδοση ή την ανανέωση πιστοποιητικού.

vii. Μη ανακτήσιμη καταστροφή ιδιωτικών κλειδιών.

β) Έκδοση πιστοποιητικών: Κλεμμένα πιστοποιητικά.

γ) Κλοπή ταυτότητας: Ο επιτιθέμενος κάνει ψευδή αξίωση ταυτότητας, αποκτά πιστοποιητικά για διαφορετική ταυτότητα.

δ) Αναίρεση αίτησης εμπιστοσύνης: σφάλμα λογισμικού ή υλικού που προκαλεί διακοπή της υπηρεσίας απόκρισης σε αίτημα ανάκλησης.

ε) Αποτυχία του παρόχου να δεχτεί ή να επεξεργαστεί τα αιτήματα ανάκλησης.

στ) Αποτυχία διάθεσης πληροφορίας για τη διαθεσιμότητα ή ανάκληση εγκεκριμένων πιστοποιητικών (μη διαθεσιμότητα της υπηρεσίας CRL/OCSP).

ζ) Ασυνέπεια μεταξύ της πληροφορίας που περιέχει η CRL και των απαντήσεων του πρωτοκόλλου OCSP.

η) Παραβιάσεις ασφαλείας που οδηγούν σε παραβίαση προσωπικών δεδομένων, πελατών ή άλλων μερών, όπως οι υπάλληλοι ή οι σύμβουλοι του παρόχου.

θ) Μη διαθεσιμότητα της υποδομής αποθήκευσης δημόσιου κλειδιού (πιστοποιητικά Root και Sub CA).

ι) Μη διαθέσιμη υπηρεσία χρονοσφραγίδας, εφόσον παρέχεται.

ια) Έκδοση χρονοσφραγίδων με λανθασμένη πληροφορία χρόνου.

ιβ) Έκδοση εγκεκριμένων πιστοποιητικών χωρίς τη χρήση αξιόπιστων συστημάτων σύμφωνα με το άρθρο 24, παρ. 2, στ. (ε) του Κανονισμού eIDAS.

ιγ) Υποβαθμισμένη ή μη διαθέσιμη υπηρεσία εμπιστοσύνης, π.χ. όπου χρησιμοποιούνται διακομιστές υπογραφής ή δίκτυο/κεντρικό σύστημα αποθήκευσης κλειδιού το οποίο τίθεται εκτός λειτουργία ή δημιουργεί υπογραφές που δεν είναι σύμφωνες με τα πρότυπα και δεν μπορούν να επικυρωθούν.

ιδ) Μη εξουσιοδοτημένη πρόσβαση σε, διαγραφή ή αλλαγή των προσωπικών δεδομένων των πελατών του παρόχου.

ιε) Περιστατικά ασφαλείας που οδηγούν σε παραβίαση της ασφάλειας των επικοινωνιών, οδηγώντας σε παραβιάσεις της ιδιωτικής ζωής.

3. Όταν συμβεί ένα περιστατικό με σημαντική επίδραση (επίπεδο 3 και άνω), ο πάροχος υποβάλλει μια αρχική και σύντομη περιγραφή του περιστατικού στην ΕΕΤΤ (αρχική δήλωση συμβάντος) εντός του πρώτου 24ώρου από τον εντοπισμό του συμβάντος και στη συνέχεια, κατά τη διερεύνηση του συμβάντος, παρέχει πιο λεπτομερείς αναφορές (ενδιάμεσες δηλώσεις, όταν υπάρχουν στοιχεία να αναφερθούν ή το αργότερο κάθε 15 ημέρες από την ημερομηνία υποβολής της αρχικής δήλωσης, και τελική δήλωση συμβάντος, όταν η διερεύνηση ολοκληρωθεί και αντιμετωπιστεί το πρόβλημα).

4. Η ελάχιστη πληροφορία που πρέπει να περιλαμβάνεται σε μια ειδοποίηση συμβάντος διαφέρει ανάλογα με το αν είναι αρχική ή ενδιάμεση/τελική και αναφέρεται στη συνέχεια:

α) <u>Αρχική δήλωση συμβάντος</u>

- Επωνυμία παρόχου υπηρεσιών εμπιστοσύνης: επωνυμία της επιχείρησης.
- Στοιχεία επικοινωνίας: Στοιχεία επικοινωνίας υπευθύνου με την ΕΕΤΤ.
- Ημερομηνία και ώρα κατά την οποία το περιστατικό ασφαλείας εντοπίστηκε (ή ξεκίνησε εάν είναι γνωστό).
- Υπηρεσίες εμπιστοσύνης που επηρεάζονται (ή πιθανώς επηρεάζονται): περιγραφή της υπηρεσίας ή των υπηρεσιών που αφορά το περιστατικό ασφαλείας.
- Σύντομη περιγραφή του συμβάντος ασφαλείας.
- Τα προσωπικά δεδομένα που επηρεάστηκαν (ή ενδεχομένως επηρεάστηκαν) και περιγραφή αυτών.
- Μέτρα που ελήφθησαν ή προγραμματίστηκαν.
- Διασυνοριακές επιπτώσεις.

β) <u>Ενδιάμεσες δηλώσεις και Τελική δήλωση συμβάντος</u>

- Επωνυμία παρόχου υπηρεσιών εμπιστοσύνης: επωνυμία της επιχείρησης.
- Στοιχεία επικοινωνίας: Στοιχεία επικοινωνίας υπευθύνου με την ΕΕΤΤ.
- Ημερομηνία και ώρα έναρξης του περιστατικού ασφαλείας.
- Ημερομηνία και ώρα που το περιστατικό ασφαλείας εντοπίστηκε από τον πάροχο.
- Διάρκεια του συμβάντος σε ώρες: η χρονική περίοδος μεταξύ της στιγμής κατά την οποία η υπηρεσία αρχίζει να υποβαθμίζεται και της στιγμής που η υπηρεσία είναι πάλι διαθέσιμη στον τελικό χρήστη ή το χρονικό διάστημα κατά το οποίο η υπηρεσία δεν ήταν διαθέσιμη στους τελικούς χρήστες.
- Σοβαρότητα του συμβάντος: Η σοβαρότητα του συμβάντος ασφαλείας, όπως ορίζεται στην παράγραφο 1 του άρθρου αυτού, όπως την εκτιμά ο πάροχος.

- Περιγραφή του συμβάντος ασφαλείας: ενδεικτικά, ποια συστήματα επηρεάζονται, πώς εντοπίστηκε το συμβάν, πόσο καιρό το περιστατικό ήταν ενεργό, αν υπάρχει ευπάθεια σε λογισμικό που περιλαμβάνει τρίτο μέρος κ.λπ.
- Υπηρεσίες εμπιστοσύνης που επηρεάζονται (ή πιθανώς επηρεάζονται): περιγραφή της υπηρεσίας ή των υπηρεσιών που επηρεάστηκαν.
- Αριθμός και ποσοστό πελατών που επηρεάστηκαν.
- Χαρακτηριστικά ασφαλείας που επηρεάζονται: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα.
- Στην περίπτωση που υπήρξε παραβίαση δεδομένων προσωπικού χαρακτήρα, τα δεδομένα προσωπικού χαρακτήρα που επηρεάστηκαν και περιγραφή αυτών.
- Λεπτομερή στοιχεία που επηρεάστηκαν: πλατφόρμα Αρχής Πιστοποίησης (CA), πλατφόρμα Αρχής Επικύρωσης (Validation Authority - VA), πλατφόρμα Αρχής Χρονοσφραγίδας (Timestamping Authority - TSA), Πλατφόρμα Αρχής Εγγραφής (Registration Authority - RA), πλατφόρμα δημιουργίας και επικύρωσης υπογραφών / σφραγίδων, πλατφόρμα διατήρησης υπογραφών / σφραγίδων, πλατφόρμα υπηρεσίας συστημένης παράδοσης, πλατφόρμα δικτύου, αρχείο, υλικό, λογισμικό, άλλα.
- Αντίκτυπος της παραβίασης ενός εκ των χαρακτηριστικών ασφαλείας (διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα) για κάθε υπηρεσία και συσχετιζόμενου στοιχείου που επηρεάστηκε: χαμηλός, μέσος, υψηλός).
- Κατηγορία αιτίας:
  - ανθρώπινο λάθος,
  - κακόβουλες ενέργειες,
  - φυσικές καταστροφές, - αποτυχία συστήματος,
  - αποτυχία τρίτων μερών.
- Λεπτομερής περιγραφή του τρόπου με τον οποίο παραβιάστηκε η ασφάλεια:
  - Επίθεση άρνησης εξυπηρέτησης (Denial of Service),
  - Κακόβουλο λογισμικό (Malware) και ιοί,
  - Κλοπή ή απώλεια εξοπλισμού,
  - Κλοπή ή απώλεια δεδομένων,
  - Διακοπή ρεύματος,
  - Αποτυχία υλικού,
  - Σφάλμα λογισμικού,
  - Ελαττωματική αλλαγή / ενημέρωση υλικού,
  - Ελαττωματική αλλαγή / ενημέρωση λογισμικού,
  - Παραβίαση προσωπικών δεδομένων,
  - Υποκλοπή,
  - Κρυπτοαναλύσεις,
  - Υπερφόρτωση,

- Εσφαλμένη πολιτική ή διαδικασία,
- Ασφάλεια τερματισμού λειτουργίας,
- Άλλα

- Εκτίμηση ζημίας που έχουν υποστεί ο πάροχος, οι συνδρομητές και τα εξαρτώμενα μέρη (Relying Parties).
- Μέτρα που ελήφθησαν για το μετριασμό του συμβάντος.
- Μακροπρόθεσμα μέτρα, που έχουν ληφθεί ή προγραμματίζονται, ώστε να αποφευχθούν παρόμοια περιστατικά στο μέλλον.
- Διασυνοριακές επιπτώσεις.
- Άλλες Αρχές που ενημερώθηκαν.
- Ειδοποίηση ενδιαφερόμενων πελατών (ΝΑΙ/ΟΧΙ, ημερομηνία και περιεχόμενο ειδοποίησης).
- Δημόσια ενημέρωση (ΝΑΙ/ΟΧΙ, ημερομηνία και περιεχόμενο ενημέρωσης).

Άρθρο 8

Υποχρέωση ενημέρωσης και καταβολής ετήσιου τέλους

1. Οι ΠΥΕ υποχρεούνται να γνωστοποιούν ηλεκτρονικά στην ΕΕΤΤ κάθε μεταβολή ή τροποποίηση των στοιχείων που περιλαμβάνονται στο Αρχείο των εγκατεστημένων στην Ελλάδα ΠΥΕ που τηρεί η ΕΕΤΤ (άρθρο 3, παρ. 1), εντός αποκλειστικής προθεσμίας ενός (1) μηνός από την επέλευσή της.
2. Οι μη εγκεκριμένοι ΠΥΕ υποχρεούνται εντός του πρώτου τριμήνου κάθε έτους να ενημερώνουν εγγράφως την ΕΕΤΤ σχετικά με την πρόθεσή τους να συνεχίσουν να παρέχουν υπηρεσίες εμπιστοσύνης και τυχόν μεταβολές των στοιχείων τους.
3. Οι εγκεκριμένοι ΠΥΕ υποχρεούνται στην καταβολή ετήσιου τέλους ύψους τριακοσίων ευρώ (€300). Το ως άνω τέλος για κάθε ημερολογιακό έτος θα καταβάλλεται εντός του τελευταίου τριμήνου του αμέσως προηγουμένου έτους.

ΜΕΡΟΣ Δ': Υποχρεώσεις μη εγκεκριμένων Παρόχων Υπηρεσιών Εμπιστοσύνης

Άρθρο 9

Υποχρέωση γνωστοποίησης τερματισμού εργασιών μη εγκεκριμένου ΠΥΕ

1. Σε περίπτωση τερματισμού των εργασιών του, εκούσιου ή ακούσιου, ένας μη εγκεκριμένος ΠΥΕ έχει τις ακόλουθες υποχρεώσεις:

   α) γνωστοποιεί άμεσα τον τερματισμό των υπηρεσιών του στην ΕΕΤΤ, στους χρήστες των υπηρεσιών εμπιστοσύνης που παρέχει και σε κάθε άλλον ΠΥΕ ή τρίτο, με τον οποίο έχει συνάψει σύμβαση ή έχει οποιαδήποτε άλλη σχέση στο πλαίσιο παροχής υπηρεσιών εμπιστοσύνης,

   β) ανακαλεί όλα τα σε ισχύ πιστοποιητικά που έχει εκδώσει και προχωρά στην οριστική καταστροφή των ιδιωτικών κλειδιών των Αρχών Πιστοποίησης της υποδομής του, εκτός κι αν προσκομίσει στην ΕΕΤΤ κατά τη γνωστοποίηση που προβλέπεται στο σημείο α) αυτής της παραγράφου, σύμβαση με άλλον ΠΥΕ, που είναι καταχωρισμένος στο αρχείο που τηρεί

η ΕΕΤΤ, βάσει της οποίας ο έτερος συμβαλλόμενος αναλαμβάνει τη συνέχιση της παροχής των υπηρεσιών του.

2. Η ΕΕΤΤ, κατόπιν της λήψης της γνωστοποίησης, καταχωρίζει τον τερματισμό εργασιών του ΠΥΕ στο αρχείο που τηρεί. Η ΕΕΤΤ δύναται προηγουμένως να ελέγξει τη συμμόρφωση με τις υποχρεώσεις που προβλέπονται στο σημείο (β) της ανωτέρω παραγράφου.

ΜΕΡΟΣ Ε': Υποχρεώσεις εγκεκριμένων Παρόχων Υπηρεσιών Εμπιστοσύνης

Άρθρο 10

Δημοσίευση πληροφοριών

1. Οι εγκεκριμένοι ΠΥΕ οφείλουν να δημοσιεύουν στον ιστότοπό τους, κατ' ελάχιστον, τα ακόλουθα:

   α) Δήλωση των πρακτικών υπηρεσίας εμπιστοσύνης (CPS),

   β) Πολιτικές κάθε υπηρεσίας εμπιστοσύνης (CP),

   γ) Σύμβαση αιτήματος παροχής υπηρεσιών και όρους χρήσης.

2. Τα έγγραφα της ανωτέρω παραγράφου δημοσιεύονται υποχρεωτικά στην Ελληνική και Αγγλική γλώσσα. Προαιρετικά μπορούν να δημοσιεύονται και σε άλλες γλώσσες.

Άρθρο 11

Τήρηση σχεδίου τερματισμού εργασιών

1. Ως Τερματισμός Εργασιών νοείται κάθε μερική έως και η πλήρης παύση μίας υπηρεσίας. Η μερική παύση μιας υπηρεσίας συμπεριλαμβάνει τη λήξη ενός ή περισσοτέρων στοιχείων που περιλαμβάνονται στον Κατάλογο Υπηρεσιών Εμπιστοσύνης στις οποίες έχει αποδοθεί το καθεστώς της έγκρισης. Οι κατηγορίες τερματισμού εργασιών μπορεί να είναι (όχι περιοριστικά):

   α) [Προγραμματισμένη] Παύση του κύκλου ζωής ή παροπλισμός των τεχνολογιών που αφορούν μία εγκεκριμένη υπηρεσία καταχωρισμένη στον Κατάλογο Υπηρεσιών Εμπιστοσύνης.

   β) [Προγραμματισμένη] Αναμενόμενη παύση υπηρεσιών (π.χ. για επιχειρηματικούς λόγους) και εξυπηρέτηση των επηρεαζόμενων συνδρομητών

      i. από τον ίδιο τον ΠΥΕ,

      ii. από άλλο εγκεκριμένο πάροχο, με μεταφορά του αρχείου του ΠΥΕ προκειμένου να είναι δυνατή η συνέχιση της παροχής της υπηρεσίας (άρθρο 12, παρ. 3, σημ. (ε)),

      iii. από την ΕΕΤΤ, με μεταφορά του αρχείου του ΠΥΕ προκειμένου να είναι δυνατή η συνέχιση της παροχής της υπηρεσίας (άρθρο 12, παρ. 3, σημ. (ε)).

   γ) [Προγραμματισμένη] Συγχώνευση ή απόκτηση δραστηριοτήτων των εν λόγω υπηρεσιών από άλλη νομική οντότητα.

   δ) [Μη προγραμματισμένη] Διακοπή λόγω καταστροφής ή λόγω άλλων σημαντικών καταστάσεων, από τις οποίες δεν υπάρχει δυνατότητα ικανοποιητικής ανάκτησης δεδομένων.

ε) [Μη προγραμματισμένη] Παύση λόγω πτώχευσης.

2. Κάθε εγκεκριμένος ΠΥΕ συντάσσει και διατηρεί ενημερωμένο Σχέδιο Τερματισμού Εργασιών, σύμφωνα με το άρθρο 24, παρ. 2, στ. (θ) του Κανονισμού eIDAS, με σκοπό την εξασφάλιση της συνέχειας της υπηρεσίας.

3. Κάθε εγκεκριμένος ΠΥΕ υποβάλλει το Σχέδιο Τερματισμού Εργασιών προς έγκριση στην ΕΕΤΤ κατά την έναρξη των εργασιών του, όπως προβλέπεται από το άρθρο 5, παρ. 4, σημ. (ιβ), καθώς και μετά από κάθε ενημέρωσή του ή σχετικού αιτήματος της ΕΕΤΤ. Το Σχέδιο Τερματισμού Εργασιών αξιολογείται από τον ΟΑΣ και η αξιολόγησή του περιλαμβάνεται στην ΕΑΣ του ΠΥΕ.

4. Η ΕΕΤΤ ελέγχει το σχέδιο τερματισμού ως προς τη συμμόρφωσή του με τον Κανονισμό eIDAS, τόσο κατά την έναρξη όσο και κατά τη διάρκεια λειτουργίας του εγκεκριμένου ΠΥΕ και των εγκεκριμένων υπηρεσιών που αυτός παρέχει. Η ΕΕΤΤ δύναται να διενεργεί ελέγχους προκειμένου να επαληθεύσει την ορθή εφαρμογή των διατάξεων του σχεδίου τερματισμού.

5. Το σχέδιο τερματισμού πρέπει να:

α) καλύπτει, κατ' ελάχιστον, την εκούσια και ακούσια διακοπή των δραστηριοτήτων, την παύση μιας, περισσότερων ή όλων των υπηρεσιών από τον πάροχο, την ενδεχόμενη ανάληψη των δραστηριοτήτων που επηρεάζονται από άλλο εγκεκριμένο ΠΥΕ,

β) διασφαλίζει τη διατήρηση και τη διαθεσιμότητα των πληροφοριών που αναφέρονται στο άρθρο 24, παρ. 2, στ. (η) του Κανονισμού eIDAS, σύμφωνα με τις διατάξεις του άρθρου αυτού,

γ) προσδιορίζει τον αντίκτυπο του τερματισμού στις σχετικές καταχωρίσεις εγκεκριμένων υπηρεσιών του Καταλόγου Υπηρεσιών Εμπιστοσύνης,

δ) προβλέπει διαδικασίες για τη διαθεσιμότητα και προσβασιμότητα των αρχείων του ΠΥΕ σύμφωνα με τις υποχρεώσεις που προβλέπονται στο άρθρο 15 της παρούσας περί τήρησης αρχείου,

ε) προβλέπει την ενημέρωση των εμπλεκομένων μερών που, ενδεχομένως, επηρεάζονται από τον τερματισμό.

6. Επιπλέον, το σχέδιο τερματισμού πρέπει να περιλαμβάνει, τουλάχιστον, τα ακόλουθα:

α) Διαδικασίες τερματισμού.

β) Διαδικασίες και σενάρια δοκιμών τερματισμού.

γ) Εκπαίδευση σε διαδικασίες τερματισμού (συμπεριλαμβανομένης της δοκιμής).

δ) Εκθέσεις δοκιμών διαδικασιών τερματισμού.

ε) Επίσημες αναφορές ελέγχου διαδικασιών τερματισμού.

στ) Επίσημες συμφωνίες τερματισμού (συμβατικές) με τρίτους (συμπεριλαμβανομένων των υπεργολάβων κ.λπ.).

ζ) Τους όρους και τις συνθήκες της εν λόγω υπηρεσίας, τις πρακτικές και τα έγγραφα πολιτικής.

7. Στο Παράρτημα 3 παρατίθεται προτεινόμενος πίνακας περιεχομένων για το σχέδιο τερματισμού.

Άρθρο 12

Υποχρέωση γνωστοποίησης τερματισμού εργασιών εγκεκριμένου ΠΥΕ

1. Σε περίπτωση τερματισμού, εκούσιου ή ακούσιου, μιας εγκεκριμένης υπηρεσίας, ένας εγκεκριμένος ΠΥΕ έχει τις ακόλουθες υποχρεώσεις:

   α) γνωστοποιεί άμεσα τον τερματισμό της εγκεκριμένης υπηρεσίας που παρέχει στην ΕΕΤΤ, στους χρήστες της και σε κάθε άλλον ΠΥΕ ή τρίτο, με τον οποίο έχει συνάψει σύμβαση ή έχει οποιαδήποτε άλλη σχέση στο πλαίσιο παροχής υπηρεσιών εμπιστοσύνης, που επηρεάζεται από τον τερματισμό της,

   β) ο ΠΥΕ φέρει το βάρος απόδειξης της γνωστοποίησης που αναφέρεται στο εδάφιο α) της παρούσας παραγράφου,

   γ) προβαίνει χωρίς καθυστέρηση στην ανάκληση όλων των σε ισχύ πιστοποιητικών που έχει εκδώσει μέσω της εν λόγω εγκεκριμένης υπηρεσίας, προχωρά στην οριστική καταστροφή των ιδιωτικών κλειδιών των Αρχών Πιστοποίησης που χρησιμοποιούνται για την παροχή της και εξασφαλίζει τη διαθεσιμότητα του συνόλου της πληροφορίας που αφορά στις εγκεκριμένες υπηρεσίες εμπιστοσύνης, σύμφωνα με το άρθρο 24, παρ. 2, στ. (η) του Κανονισμού eIDAS,

2. Η ΕΕΤΤ, κατόπιν της λήψης της γνωστοποίησης της ανωτέρω παραγράφου, προχωρά στην ενημέρωση του Καταλόγου Υπηρεσιών Εμπιστοσύνης. Η ΕΕΤΤ δύναται προηγουμένως να ελέγξει τη συμμόρφωση με τις υποχρεώσεις που προβλέπονται στο σημείο γ) της ανωτέρω παραγράφου.

3. Σε περίπτωση τερματισμού, εκούσιου ή ακούσιου, του συνόλου των εργασιών του, ένας εγκεκριμένος ΠΥΕ έχει τις ακόλουθες υποχρεώσεις:

   α) γνωστοποιεί άμεσα την πρόθεσή του να τερματίσει την παροχή των υπηρεσιών του στην ΕΕΤΤ, στους χρήστες των υπηρεσιών εμπιστοσύνης που παρέχει και σε κάθε άλλον ΠΥΕ ή τρίτο, με τον οποίο έχει συνάψει σύμβαση ή έχει οποιαδήποτε άλλη σχέση στο πλαίσιο παροχής υπηρεσιών εμπιστοσύνης,

   β) σε περιπτώσεις για τις οποίες προϋποτίθεται η έκδοση δικαστικής απόφασης για την επέλευση της παύσης των εργασιών του ΠΥΕ, ο τελευταίος οφείλει να ενημερώσει την ΕΕΤΤ από την επομένη της επίδοσης στον ΠΥΕ ή κατάθεσης από τον ΠΥΕ κάθε δικογράφου σχετικού με τον τερματισμό των εργασιών του. Με την έκδοση και δημοσίευση της σχετικής απόφασης, ο ΠΥΕ υποχρεούται να ενημερώσει όσους αναφέρονται στο εδάφιο α) της παρούσας παραγράφου,

   γ) σε κάθε περίπτωση, ο ΠΥΕ φέρει το βάρος απόδειξης της γνωστοποίησης που αναφέρεται στο εδάφιο α) της παρούσας παραγράφου,

   δ) στην περίπτωση που δεν είναι δυνατόν για έναν εγκεκριμένο ΠΥΕ να μεταφέρει τις δραστηριότητες σε άλλο εγκεκριμένο Πάροχο για τη συνέχιση των εγκεκριμένων υπηρεσιών που παρέχει από αυτόν, ο ΠΥΕ προβαίνει άμεσα στην ανάκληση όλων των σε ισχύ πιστοποιητικών που έχει εκδώσει, προχωρά στην οριστική καταστροφή των ιδιωτικών κλειδιών των Αρχών Πιστοποίησης της υποδομής του και εξασφαλίζει τη διαθεσιμότητα του συνόλου της πληροφορίας που αφορά στις εγκεκριμένες υπηρεσίες εμπιστοσύνης, σύμφωνα με το άρθρο 24, παρ. 2, στ. (η) του Κανονισμού eIDAS, όπως ορίζεται στο σημείο ε) κατωτέρω,

   ε) ο ΠΥΕ Εγκεκριμένων Πιστοποιητικών, σε κάθε περίπτωση, υποχρεούται να έχει ήδη συμφωνήσει εγγράφως με άλλον εγκεκριμένο ΠΥΕ, για την παράδοση στον τελευταίο του

αρχείου που τηρεί, σύμφωνα με το άρθρο 15 της παρούσας. Ο ΠΥΕ – δέκτης, ο οποίος σύμφωνα με τα ανωτέρω παραλαμβάνει και διατηρεί το αρχείο του ΠΥΕ – δότη λόγω την παύσης των εργασιών του τελευταίου, οφείλει το αργότερο επτά (7) ημέρες πριν την ανάληψη του αρχείου να κοινοποιεί εγγράφως στην ΕΕΤΤ το γεγονός αυτό. Σε περίπτωση μη εφαρμογής των ανωτέρω και χωρίς περιορισμό τους, ο ΠΥΕ του οποίου οι εργασίες παύουν, παραδίδει τα εν λόγω έγγραφα και στοιχεία προς φύλαξη στην ΕΕΤΤ, ενημερώνοντας σχετικά τους χρήστες των υπηρεσιών εμπιστοσύνης που παρέχει.

στ) σε κάθε περίπτωση, οι τυχόν συμβάσεις ανάθεσης σε τρίτους εκτέλεσης μέρους της διαδικασίας παροχής υπηρεσιών εμπιστοσύνης, λήγουν αυτοδικαίως με την παύση εργασιών του ΠΥΕ. Για το σκοπό αυτό, οι συμβάσεις οι οποίες υπογράφονται μεταξύ ΠΥΕ και τρίτων, οφείλουν να περιλαμβάνουν όρους με τους οποίους να διασφαλίζεται η εκ μέρους των τρίτων παράδοση του αρχείου και όλων των σχετικών εγγράφων, σύμφωνα με το σημείο (ε) της παρούσας παραγράφου,

ζ) ο ΠΥΕ υποχρεούται να έχει ρυθμίσει την οικονομική κάλυψη κάθε απαιτούμενης διαδικασίας και εκπλήρωσης υποχρεώσεων που προκύπτουν από τον τερματισμό των εργασιών του καθώς και ενδεχόμενης ζημίας που τυχόν προκληθεί σε χρήστες των υπηρεσιών εμπιστοσύνης που παρέχει ή σε τρίτους από ενέργεια ή παράλειψή του, κατά την άσκηση των δραστηριοτήτων του, και ειδικότερα, συνεπεία του τερματισμού εργασιών του. Ο ΠΥΕ οφείλει να είναι σε θέση να αποδείξει στην ΕΕΤΤ και σε οποιονδήποτε έχει έννομο συμφέρον ότι έχει προβλέψει επαρκώς για την ως άνω αναφερόμενη οικονομική κάλυψη,

4. Η ΕΕΤΤ, κατόπιν της λήψης της γνωστοποίησης από τον εγκεκριμένο ΠΥΕ ή από οποιονδήποτε εξουσιοδοτημένο τρίτο (π.χ. σε περίπτωση μη αναμενόμενου τερματισμού ή πτώχευσης), περί του επελθόντος ή επικείμενου τερματισμού παροχής των υπηρεσιών εν μέρει ή εξ ολοκλήρου, ελέγχει και επαληθεύει την ορθή εφαρμογή του σχεδίου τερματισμού, συμπεριλαμβανομένου του τρόπου με τον οποίο οι πληροφορίες παραμένουν προσβάσιμες σύμφωνα με το άρθρο 24, παρ. 2, στ. (η) του Κανονισμού eIDAS, και προχωρά στην κατάλληλη ενημέρωση του Καταλόγου Υπηρεσιών Εμπιστοσύνης.

5. Για την ορθή εφαρμογή του τερματισμού, ο εγκεκριμένος ΠΥΕ οφείλει να μεριμνήσει για την κατάλληλη κοινοποίηση της πρόθεσής του, τη διαφύλαξη του συνόλου της πληροφορίας που αφορά στα εκδοθέντα εγκεκριμένα πιστοποιητικά και τη διαθεσιμότητα της CRL ή της υπηρεσίας OCSP, για επτά (7) έτη από τη λήξη τους, ακόμη και μετά την παύση των δραστηριοτήτων του. Επίσης όλες οι σχετικές πληροφορίες σχετικά με τα δεδομένα που εκδίδονται και λαμβάνονται από τον ΠΥΕ, πρέπει να είναι διαθέσιμες ανά πάσα στιγμή, ιδίως για να παρέχονται ως αποδεικτικά στοιχεία σε δικαστικές διαδικασίες και με σκοπό τη διασφάλιση της συνέχειας της υπηρεσίας.

6. Η ανάλυση του κινδύνου μη ορθής εκτέλεσης του σχεδίου τερματισμού πρέπει να περιλαμβάνεται στην αναφορά αποτίμησης κινδύνου που προβλέπεται στο άρθρο 5, παρ.4, σημ. (ι).

Άρθρο 13

Υποχρέωση υποβολής έκθεσης αξιολόγησης συμμόρφωσης

1. Οργανισμοί Αξιολόγησης Συμμόρφωσης (ΟΑΣ), σύμφωνα με τον Κανονισμό eIDAS, είναι φορείς που έχουν διαπιστευθεί σύμφωνα με τον Κανονισμό (ΕΚ) αριθ. 765/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για τον καθορισμό των απαιτήσεων διαπίστευσης και εποπτείας από την αγορά σε σχέση με την εμπορία των

προϊόντων και κατάργηση του κανονισμού (ΕΟΚ) αριθ. 339/93, ως κατάλληλοι για τη διενέργεια ελέγχων συμμόρφωσης εγκεκριμένων ΠΥΕ και των εγκεκριμένων υπηρεσιών που αυτοί παρέχουν. Η διαπίστευση χορηγείται από τον Εθνικό Φορέα Διαπίστευσης του κράτους στο οποίο είναι εγκατεστημένος ο ΟΑΣ ή από Φορέα Διαπίστευσης άλλου Κράτους Μέλους και πρέπει να πιστοποιεί ότι ο ΟΑΣ:

α) έχει την ικανότητα και επαρκείς γνώσεις για την αξιολόγηση ΠΥΕ ως προς τις απαιτήσεις του κανονισμού eIDAS και

β) προσαρμόζεται στις απαιτήσεις του προτύπου ISO/IEC 17065: 2012 και των προτύπων ETSI TS 119 403-3 και ETSI EN 319 403-1 ή άλλου ισοδύναμου προτύπου. Μεταβατικά, μέχρι 31/12/2022, αρκεί να προσαρμόζεται στις απαιτήσεις του προτύπου ISO/IEC 17065: 2012 και του προτύπου ETSI EN 319 403.

Ο ΟΑΣ υποχρεούται να παράσχει όλες τις απαιτούμενες διευκρινίσεις στην ΕΕΤΤ σχετικά με το πλήρες σχήμα πιστοποίησης, που εφαρμόζει, κατόπιν σχετικού αιτήματος της ΕΕΤΤ.

2. Η υποχρέωση ελέγχου των εγκεκριμένων ΠΥΕ ορίζεται στο άρθρο 20, παρ. 1 του Κανονισμού eIDAS. Επιπλέον, η διενέργεια ελέγχου απαιτείται στις ακόλουθες περιπτώσεις:

α) Κατά την έναρξη εγκεκριμένων υπηρεσιών εμπιστοσύνης (άρθρο 5 της παρούσας).

β) Κατά την ενεργοποίηση μιας νέας εγκεκριμένης υπηρεσίας από αυτές που προβλέπονται στον Κανονισμό eIDAS για την οποία ο ΠΥΕ δεν έχει λάβει προηγούμενη έγκριση από την ΕΕΤΤ.

γ) Κατά την ένταξη μιας νέας Αρχής Εγγραφής, εφόσον απαιτηθεί από την ΕΕΤΤ.

δ) Κατά την ενεργοποίηση υπηρεσίας απομακρυσμένης ηλεκτρονικής υπογραφής ή σφραγίδας.

ε) Κατόπιν σχετικού αιτήματος της ΕΕΤΤ σε κάθε περίπτωση.

3. Μετά την ολοκλήρωση του ελέγχου του εγκεκριμένου ΠΥΕ, ο ΟΑΣ εκδίδει Έκθεση Αξιολόγησης Συμμόρφωσης (ΕΑΣ), την οποία υπογράφουν οι έχοντες κατάλληλη εξουσιοδότηση με εγκεκριμένη ηλεκτρονική υπογραφή. Αυτή είναι μία λεπτομερής αναφορά που περιέχει όλα τα αποτελέσματα της αξιολόγησης που έχει εκτελεστεί και, με εξαίρεση την περίπτωση που ο έλεγχος έχει ζητηθεί από την ΕΕΤΤ σύμφωνα με το άρθρο 20, παρ. 2 του Κανονισμού eIDAS, παραδίδεται στον ελεγχόμενο ΠΥΕ. Ο ΠΥΕ υποβάλλει υποχρεωτικά εντός τριών (3) εργάσιμων ημερών την ΕΑΣ στην ΕΕΤΤ.

4. Η ΕΑΣ μπορεί να βασίζεται σε επιμέρους ΕΑΣ που έχουν υποβληθεί από εγκεκριμένους ΠΥΕ ή τρίτους για κάποια επιμέρους υπηρεσία (π.χ. Αρχή Εγγραφής) και έχουν εγκριθεί από την ΕΕΤΤ, χωρίς να χρειάζεται να επανελεγχθούν τα στοιχεία της υπηρεσίας των οποίων η συμμόρφωση με τις απαιτήσεις του Κανονισμού eIDAS έχει πιστοποιηθεί με τις συγκεκριμένες επιμέρους ΕΑΣ. Στην περίπτωση αυτή, η διάρκεια ισχύος της ΕΑΣ που υποβάλλεται δεν μπορεί να υπερβαίνει το διάστημα κατά το οποίο ισχύουν όλες οι επιμέρους ΕΑΣ στις οποίες βασίζεται.

5. Η ΕΑΣ αφορά αποκλειστικά σε έναν και μόνο ΠΥΕ.

6. Ο σκοπός της ΕΑΣ δεν είναι να επιβεβαιώσει ότι ο εγκεκριμένος ΠΥΕ και οι εγκεκριμένες υπηρεσίες που παρέχει ακολουθούν συγκεκριμένα τεχνικά πρότυπα, αλλά ότι είναι σε συμμόρφωση με τον Κανονισμό eIDAS. Η συμμόρφωση με τεχνικά πρότυπα μπορεί σε κάποιες περιπτώσεις να συνεπάγεται τη συμμόρφωση με κάποιες απαιτήσεις του Κανονισμού eIDAS, αλλά δεν είναι υποχρεωτική. Συστήνεται η παρακολούθηση των ευρωπαϊκών

προτύπων (ETSI, European Telecommunications Standards Institute και CEN, European Committee for Standardisation) για να εξασφαλίζεται η διαλειτουργικότητα των υπηρεσιών που παρέχουν οι εγκεκριμένοι ΠΥΕ.

7. Μετά από έλεγχο της ΕΑΣ για τη διαπίστωση της συμμόρφωσης του ΠΥΕ και των υπηρεσιών που παρέχει με τις απαιτήσεις του Κανονισμού eIDAS, η ΕΕΤΤ εκδίδει απόφαση για την απόδοση ή διατήρηση του καθεστώτος του εγκεκριμένου παρόχου στον ΠΥΕ και την έγκριση των υπηρεσιών που παρέχει ή νέων. Η ΕΕΤΤ ολοκληρώνει τον έλεγχο και εκδίδει απόφαση εντός τριών (3) μηνών από την υποβολή της ΕΑΣ, διαφορετικά ενημερώνει τον ΠΥΕ για τους λόγους της καθυστέρησης και το χρόνο εντός του οποίου αναμένεται να ολοκληρωθεί η διαδικασία. Σε περίπτωση απόρριψης του αιτήματος, ο ΠΥΕ υποχρεούται να ενημερώσει εντός επτά (7) εργασίμων ημερών τον ΟΑΣ προκειμένου να αποσύρει τη δημοσίευση οποιουδήποτε πιστοποιητικού συμμόρφωσης, στην οποία ενδεχομένως έχει προχωρήσει βάσει της εκδοθείσας ΕΑΣ, ενημερώνοντας την ΕΕΤΤ μετά την ολοκλήρωση των σχετικών ενεργειών του ΟΑΣ. Μετά την ολοκλήρωση του ελέγχου, η ΕΕΤΤ ενημερώνει κατάλληλα τον Κατάλογο Υπηρεσιών Εμπιστοσύνης, εφόσον απαιτείται.

Άρθρο 14

Περιεχόμενο της ΕΑΣ

Με την επιφύλαξη ότι η ΕΕΤΤ δύναται να ζητήσει πρόσθετα στοιχεία και πληροφορίες από τον ΠΥΕ, η ΕΑΣ πρέπει να περιλαμβάνει τουλάχιστον τα στοιχεία που αναφέρονται κατωτέρω. Ως προς την εμπιστευτικότητα των υποβληθέντων στοιχείων, ισχύουν οι διατάξεις της ενωσιακής και της εθνικής νομοθεσίας περί εμπορικού απορρήτου και περί προστασίας προσωπικών δεδομένων.

α) Στοιχεία του ΟΑΣ: επωνυμία, ταχυδρομική διεύθυνση της έδρας του, στοιχεία εγγραφής σε δημόσια αρχεία (π.χ. Γ.Ε.ΜΗ., ΑΦΜ) και δεδομένα επικοινωνίας του νομίμου εκπροσώπου (αριθμός τηλεφώνου και διεύθυνση ηλεκτρονικού ταχυδρομείου).

β) Στοιχεία του Φορέα Διαπίστευσης που έχει διαπιστεύσει τον ΟΑΣ: επωνυμία, ταχυδρομική διεύθυνση της έδρας του και διεύθυνση ηλεκτρονικού ταχυδρομείου καθώς και πληροφορίες που αφορούν στο πιστοποιητικό διαπίστευσης (π.χ. αριθμό αναγνώρισης του πιστοποιητικού) καθώς και σύνδεσμο στον ιστότοπο του φορέα όπου δημοσιεύεται το πιστοποιητικό διαπίστευσης.

γ) Το πιστοποιητικό του ΟΑΣ (διαπίστευση) και λεπτομερή περιγραφή του συστήματος διαπίστευσης που χρησιμοποιήθηκε, συμπεριλαμβανομένης της δήλωσης συμμόρφωσης με τις απαιτήσεις του κανονισμού eIDAS.

δ) Στοιχεία του αρμόδιου συντάκτη της ΕΑΣ (αριθμός τηλεφώνου και διεύθυνση ηλεκτρονικού ταχυδρομείου).

ε) Στοιχεία του εγκεκριμένου ΠΥΕ: όνομα/επωνυμία, τον αριθμό μητρώου στο αρχείο που τηρεί η ΕΕΤΤ αλλιώς τον ΑΦΜ του, και τη διεύθυνση επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου.

στ) Αναλυτική λίστα των εγκεκριμένων ή υπό έγκριση υπηρεσιών, για τις οποίες ο ΟΑΣ βεβαιώνει ότι πληρούν τις απαιτήσεις του Κανονισμού eIDAS. Οι υπηρεσίες καταγράφονται με βάση το αναγνωριστικό του τύπου της υπηρεσίας (Service type identifier), σύμφωνα με την απόφαση της Επιτροπής (ΕΕ) 2015/1505 και την παράγραφο 5.5.1.1 του προτύπου ETSI TS 119 612 V2.1.1 και, ακολούθως, την ψηφιακή ταυτότητα κάθε υπηρεσίας (Service digital identity, παρ. 5.5.3 ETSI TS 119

612 V2.1.1). Η καταγραφή πρέπει να περιλαμβάνει, επίσης, το αναγνωριστικό κλειδιού (Subject Key Identifier), σύμφωνα με το πρότυπο RFC 5280, και το πιστοποιητικό X.509 V3 που χρησιμοποιεί η υπηρεσία στη μορφή Base64 PEM. Εφόσον απαιτείται, περιλαμβάνεται αναφορά σε κατηγορίες τελικών πιστοποιητικών που εξαιρούνται από τον έλεγχο ή δεν καλύπτονται από την απόφαση πιστοποίησης καθώς και τα κριτήρια βάσει των οποίων αυτά μπορούν να προσδιοριστούν. Επιπλέον, αναφέρεται αν η ψηφιακή ταυτότητα αφορά σε υπηρεσία Αρχή Πιστοποίησης Ρίζας ή σε Υποκείμενη Αρχή Πιστοποίησης.

ζ) Για κάθε υπηρεσία της λίστας υπό στ), περιγραφή της φυσικής, λογικής και λειτουργικής αρχιτεκτονικής (ενδεικτικά, απεικόνιση της ιεραρχίας PKI με τις ΑΠ Ρίζας, τις ενδιάμεσες ΑΠ και τις ΑΠ που εκδίδουν τελικά πιστοποιητικά, χαρακτηρισμό κάθε ΑΠ μέσω του αναγνωριστικού της κλειδιού και συμπερίληψη ένδειξης σε κάθε ΑΠ που εκδίδει τελικά πιστοποιητικά για το αν αυτά είναι εγκεκριμένα ή όχι, αν προορίζονται για χρήση ηλεκτρονικής υπογραφής, σφραγίδας ή βεβαίωσης γνησιότητας ιστοτόπου ή για άλλη χρήση, με περιγραφή της χρήσης στην περίπτωση αυτή.

η) Κατάλογο των πιστοποιήσεων για την υπό εξέταση υπηρεσία ή προϊόν που χρησιμοποιεί ο Πάροχος, συμπεριλαμβανομένου ενός αντιγράφου ή συνδέσμου (link) σε αυτές.

θ) Κατάλογο των εγκεκριμένων διατάξεων δημιουργίας ηλεκτρονικής υπογραφής ή/και σφραγίδας (ΕΔΔΥ) που χρησιμοποιούνται, ο οποίος περιλαμβάνει αντίγραφο ή σύνδεσμο της πιστοποίησης που έχει εκδοθεί σύμφωνα με το άρθρο 30, παρ. 1 του Κανονισμού eIDAS ή σύνδεσμο στην πληροφορία που δημοσιεύει η Ευρωπαϊκή Επιτροπή, σύμφωνα με το άρθρο 30, παρ. 2 του Κανονισμού eIDAS, που περιλαμβάνει τη συγκεκριμένη συσκευή.

ι) Στην περίπτωση που ο Πάροχος παρέχει απομακρυσμένη υπηρεσία εγκεκριμένης ηλεκτρονικής υπογραφής, περιλαμβάνεται το αποτέλεσμα του ελέγχου των διαδικασιών που ακολουθούνται, των μηχανισμών διαχείρισης ασφάλειας, των αξιόπιστων συστημάτων και προϊόντων που χρησιμοποιούνται, συμπεριλαμβανομένης της χρήσης ασφαλών διαύλων ηλεκτρονικής επικοινωνίας για τη διασφάλιση ότι το περιβάλλον της ηλεκτρονικής υπογραφής είναι αξιόπιστο και ότι ο υπογράφων έχει υψηλό επίπεδο εμπιστοσύνης και τον αποκλειστικό έλεγχο της χρήσης δεδομένων δημιουργίας ηλεκτρονικής υπογραφής. Επίσης, περιλαμβάνεται κατάλογος των εγκεκριμένων διατάξεων εξ αποστάσεως δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιεί ο ΠΥΕ, οι οποίες έχουν πιστοποιηθεί σύμφωνα με την Εκτελεστική Απόφαση (ΕΕ) 2016/650 της Επιτροπής της 25ης Απριλίου 2016, ή τυχόν άλλη πράξη της Επιτροπής που εκδοθεί σε εφαρμογή του άρθρου 30, παρ. 3 του Κανονισμού eIDAS.

ια) Στην περίπτωση που ο Πάροχος παρέχει απομακρυσμένη υπηρεσία εγκεκριμένης ηλεκτρονικής σφραγίδας, περιλαμβάνεται το αποτέλεσμα του ελέγχου των διαδικασιών που ακολουθούνται, των μηχανισμών διαχείρισης ασφάλειας, των αξιόπιστων συστημάτων και προϊόντων που χρησιμοποιούνται, συμπεριλαμβανομένης της χρήσης ασφαλών διαύλων ηλεκτρονικής επικοινωνίας για τη διασφάλιση ότι το περιβάλλον της ηλεκτρονικής σφραγίδας είναι αξιόπιστο και ότι ο χρήστης έχει υψηλό επίπεδο εμπιστοσύνης και τον αποκλειστικό έλεγχο της χρήσης δεδομένων δημιουργίας ηλεκτρονικής σφραγίδας. Επίσης, περιλαμβάνεται κατάλογος των εγκεκριμένων διατάξεων εξ αποστάσεως δημιουργίας ηλεκτρονικής σφραγίδας που χρησιμοποιεί ο ΠΥΕ, οι οποίες έχουν πιστοποιηθεί σύμφωνα με την Εκτελεστική Απόφαση (ΕΕ) 2016/650 της Επιτροπής της 25ης Απριλίου 2016, ή τυχόν άλλη πράξη της Επιτροπής που εκδοθεί σε εφαρμογή του άρθρου 30 παρ. 3 του Κανονισμού eIDAS.

ιβ) Στην περίπτωση που η ΕΑΣ βασίζεται σε επιμέρους ΕΑΣ που έχουν εγκριθεί από την ΕΕΤΤ, αναλυτική λίστα των επιμέρους ΕΑΣ, της ημερομηνίας λήξης καθεμίας από αυτές και των σχετικών εγκριτικών Αποφάσεων της ΕΕΤΤ.

ιγ) Λεπτομερή κατάλογο όλων των εγγράφων του Παρόχου, δημόσιων και εσωτερικών, συμπεριλαμβανομένου του αριθμού έκδοσης, τα οποία ελέγχθηκαν από τον ΟΑΣ. Τα έγγραφα αυτά συνυποβάλλονται από τον Πάροχο στην ΕΕΤΤ κατά την υποβολή της ΕΑΣ εφόσον έχουν τροποποιηθεί από την τελευταία τους υποβολή. Ο κατάλογος αυτός πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα:

i. Δήλωση των πρακτικών υπηρεσίας εμπιστοσύνης (CPS).

ii. Πολιτικές κάθε υπηρεσίας εμπιστοσύνης (CP).

iii. Σχέδιο παύσης δραστηριοτήτων που αναφέρεται στο άρθρο 24, παρ. 2, στ. (θ) του Κανονισμού eIDAS και στο άρθρο 11 της παρούσας.

iv. Σύμβαση αιτήματος παροχής υπηρεσιών και όροι χρήσης.

v. Αναφορά αποτίμησης κινδύνου σύμφωνα με τις απαιτήσεις του Άρθρου 19, παρ. 1 του Κανονισμού eIDAS.

ιδ) Πίνακα με το χρονικό διάστημα ισχύος της ΕΑΣ, τους πόρους που χρησιμοποιήθηκαν για κάθε φάση του ελέγχου (επιτόπιος ή απομακρυσμένος) σε ανθρωποώρες και το επίπεδο εμπειρίας κάθε ελεγκτή, το αναλυτικό χρονοδιάγραμμα του ελέγχου, καθώς και την εργασία κάθε ελεγκτή. Το χρονοδιάγραμμα και οι πόροι που χρησιμοποιήθηκαν πρέπει να είναι ανάλογα του εύρους του ελέγχου και της εμπειρίας των ελεγκτών που διενέργησαν τον έλεγχο.

ιε) Για καθεμία από τις ακόλουθες απαιτήσεις του Κανονισμού eIDAS, αναγράφεται ο τρόπος συμμόρφωσης του Παρόχου, καθώς και αναλυτική λίστα με τα σημεία ελέγχου και των στόχων που χρησιμοποιούνται στον έλεγχο, διευκρινίζοντας, κατά περίπτωση, τις αδυναμίες συμμόρφωσης και τη σοβαρότητα αυτών, και το επίπεδο συνάφειας:

i. Γενικές απαιτήσεις

Άρθρο 13: Ευθύνη και βάρος αποδείξεως, και ειδικότερα:

i. Όρια ευθύνης

ii. Όρια όσον αφορά στις πιθανές χρήσεις των υπηρεσιών

Άρθρο 15: Προσβασιμότητα για άτομα με αναπηρίες

Άρθρο 19: Απαιτήσεις ασφάλειας για τους ΠΥΕ

ii. Ειδικές απαιτήσεις για τους εγκεκριμένους ΠΥΕ:

Άρθρο 23: Χρήση του ενωσιακού σήματος εμπιστοσύνης για τις εγκεκριμένες υπηρεσίες εμπιστοσύνης (σύμφωνα και με την Εκτελεστική Απόφαση (ΕΕ) 2015/806).

Άρθρο 24: Απαιτήσεις για τους εγκεκριμένους ΠΥΕ

iii. Δημιουργία εγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής

Άρθρο 28: Εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών

Άρθρο 29: Απαιτήσεις για τις εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής υπογραφής

iv. Δημιουργία εγκεκριμένου πιστοποιητικού ηλεκτρονικής σφραγίδας

Άρθρο 38: Εγκεκριμένα πιστοποιητικά ηλεκτρονικής σφραγίδας

Άρθρο 39: Εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής σφραγίδας

v. Δημιουργία εγκεκριμένου πιστοποιητικού ηλεκτρονικής χρονοσφραγίδας

Άρθρο 42: Απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές χρονοσφραγίδες

vi. Επικύρωση εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων

Άρθρο 32: Απαιτήσεις για την επικύρωση εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων (άρθρο 40) Άρθρο 33: Εγκεκριμένη υπηρεσία επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων (άρθρο 40)

vii. Διαφύλαξη εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων

Άρθρο 34: Εγκεκριμένη υπηρεσία διαφύλαξης εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων (άρθρο 40)

viii. Εγκεκριμένη υπηρεσία συστημένης παράδοσης

Άρθρο 44: Απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές υπηρεσίες συστημένης παράδοσης

ix. Δημιουργία εγκεκριμένου πιστοποιητικού πιστοποίησης γνησιότητας ιστοτόπων

Άρθρο 45: Απαιτήσεις για εγκεκριμένα πιστοποιητικά γνησιότητας ιστοτόπου

ιστ) Όταν η συμμόρφωση αξιολογείται περαιτέρω, σύμφωνα με συγκεκριμένα πρότυπα (π.χ. ευρωπαϊκά πρότυπα ETSI EN 319 401 / ETSI EN 319 411-1 / ETSI EN 319 411-2 / ETSI EN 319 421 κ.λπ.), αναλυτική λίστα με ρητή ένδειξη των μη συμμορφώσεων και της συνάφειάς τους.

ιζ) Σύνοψη με τα αποτελέσματα του ελέγχου του Σχεδίου Τερματισμού του ΠΥΕ.

ιη) Αναλυτικός κατάλογος τρίτων μερών στα οποία έχουν εκχωρηθεί πλήρως ή μερικώς αρμοδιότητες παροχής υπηρεσιών εμπιστοσύνης ή οι υπηρεσίες τους χρησιμοποιούνται από τον ΠΥΕ για την παροχή υπηρεσιών εμπιστοσύνης, κατόπιν σύμβασης, ο οποίος περιλαμβάνει, τουλάχιστον, το όνομα/επωνυμία του τρίτου μέρους, τον αριθμό της σύμβασης (εφόσον αυτός υπάρχει), το είδος των υπηρεσιών που παρέχει και ρητή δήλωση του ΟΑΣ σχετικά με τη συμπερίληψή τους στον έλεγχο και σε ποιο βαθμό ελέγχθηκαν.

ιθ) Σύνοψη με τα σημεία στα οποία δεν υπάρχει συμμόρφωση, αναφορά του επιπέδου σοβαρότητας (κρίσιμη ή όχι) με αιτιολόγηση.

κ) Ρητή δήλωση του αποτελέσματος του ελέγχου και της συμμόρφωσης ή μη του ΠΥΕ με τις απαιτήσεις του Κανονισμού eIDAS.

κα) Πιθανές συστάσεις προς τον ΠΥΕ.

κβ) Τυχόν απαιτούμενοι προγραμματισμένοι επιπλέον έλεγχοι που πρόκειται να πραγματοποιήσει ο ΟΑΣ (π.χ. για τον έλεγχο υλοποίησης μη-κρίσιμης σύστασης).

κγ) Ημερομηνία επόμενου ελέγχου.

κδ) Ρητή δήλωση ότι η ΕΑΣ και τα σχετικά πιστοποιητικά που εκδίδονται από τον ΟΑΣ προορίζονται για χρήση από τον Εποπτικό Φορέα (ΕΕΤΤ).

Άρθρο 15

Υποχρέωση τήρησης αρχείου

1. Κάθε εγκεκριμένος ΠΥΕ τηρεί, τουλάχιστον σε ηλεκτρονική μορφή, αρχείο με το σύνολο των πληροφοριών σχετικά με τα εγκεκριμένα πιστοποιητικά που εκδίδει ή/και διαχειρίζεται, σύμφωνα με το άρθρο 24, παρ. 2, στ) και η) του Κανονισμού eIDAS. Σε αυτά περιλαμβάνονται στοιχεία για το χρόνο έκδοσης, ακύρωσης ή αναστολής και λήξης αυτών, προκειμένου να καθίσταται δυνατή η επιβεβαίωση της ορθότητας και της ακρίβειάς τους, αλλά και στοιχεία που αφορούν στην ταυτοποίηση του κατόχου του πιστοποιητικού (τρόπος ταυτοποίησης, έγγραφο ταυτοποίησης, Αρχή Εγγραφής που έκανε την ταυτοποίηση, ημερομηνία και ώρα που έλαβε χώρα η ταυτοποίηση, ονοματεπώνυμο υπαλλήλου που διενήργησε την ταυτοποίηση κ.λπ.) και στο μοντέλο της ΕΔΔΥ που χρησιμοποιείται για την αποθήκευση του εγκεκριμένου πιστοποιητικού. Οι πληροφορίες αυτές πρέπει να είναι διαθέσιμες ανά πάσα στιγμή, ιδίως για να παρέχονται ως αποδεικτικά στοιχεία σε δικαστικές διαδικασίες αλλά και για τη διασφάλιση της συνέχειας της υπηρεσίας.
2. Κάθε εγκεκριμένο πιστοποιητικό, αμέσως μετά την έκδοσή του, καταχωρίζεται σε ηλεκτρονική μορφή στο Αρχείο, κατά τρόπο ώστε να καθίσταται δυνατός ο εντοπισμός οποιασδήποτε μεταγενέστερης αλλοίωσής του.
3. Κάθε ΠΥΕ παρέχει στο δικαιούχο του πιστοποιητικού πρόσβαση στα δεδομένα που τον αφορούν, κατόπιν υποβολής σχετικού αιτήματός του, στο οποίο ο ΠΥΕ υποχρεούται να απαντήσει εντός αποκλειστικής προθεσμίας επτά (7) εργασίμων ημερών από την ημερομηνία υποβολής του αιτήματος.
4. Κατόπιν αιτήματος ή εντολής δικαστικών ή άλλων αρμόδιων Αρχών, ο ΠΥΕ οφείλει να παρέχει πρόσβαση στο έντυπο ή/και ηλεκτρονικό αρχείο του.
5. Σε περίπτωση εγκεκριμένου πιστοποιητικού για το οποίο χρησιμοποιείται ψευδώνυμο, αντί του ονόματος του προσώπου, ο ΠΥΕ επιτρέπεται να γνωστοποιεί στοιχεία για την εξουσία εκπροσώπησης ενός τρίτου προσώπου ή επίσημα, επαγγελματικά ή άλλα στοιχεία της ταυτότητας του προσώπου, μόνο εφόσον το τρίτο πρόσωπο ή η αρμόδια αρχή έχουν συναινέσει ως προς τη χρήση του ψευδωνύμου.
6. Κάθε καταχώριση εγκεκριμένου πιστοποιητικού διατηρείται στο Αρχείο για χρονική περίοδο τουλάχιστον επτά (7) ετών από τη λήξη ισχύος του εγκεκριμένου πιστοποιητικού.

Άρθρο 16

Συμμόρφωση με τον Κανονισμό ΕΕ/2016/2019 και τον ν. 4624/2019 (Α 137)

1. Οι ΠΥΕ υποχρεούνται να τηρούν τις υποχρεώσεις που απορρέουν από την εφαρμογή του Κανονισμού (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός Προστασίας Δεδομένων / General Data Protection Regulation – GDPR) και του Ν. 4624/2019.

2. Οι ΠΥΕ επιτρέπεται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα των φυσικών προσώπων για τα οποία εκδίδουν εγκεκριμένα πιστοποιητικά για ηλεκτρονικές υπογραφές ή άλλες υπηρεσίες εμπιστοσύνης, μόνον εφόσον αυτό είναι απαραίτητο:

α) για την αποτροπή απειλών κατά της εθνικής ασφάλειας ή της δημόσιας ασφάλειας κατόπιν αιτήματος δημόσιου φορέα· ή

β) για τη δίωξη ποινικών αδικημάτων· ή

γ) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, εκτός και εάν υπερτερεί το συμφέρον του υποκειμένου των δεδομένων να μην τύχουν επεξεργασίας τα δεδομένα αυτά.

Ο ΠΥΕ έχει υποχρέωση να καταγράψει την εν λόγω γνωστοποίηση των δεδομένων και να ενημερώσει σχετικά τον δικαιούχο του πιστοποιητικού.

Μέρος ΣΤ' : Ευθύνη και εποπτεία

Άρθρο 17

Αστική ευθύνη των παρόχων υπηρεσιών εμπιστοσύνης 1. Οι ΠΥΕ που κατά υπαίτια παράβαση των διατάξεων του Κανονισμού eIDAS, του Ν. 4727/2020 ή της παρούσας, προκαλούν περιουσιακή βλάβη σε οποιοδήποτε φυσικό ή νομικό πρόσωπο υποχρεούνται σε πλήρη αποζημίωσή του. Σε περίπτωση ηθικής βλάβης, υποχρεούνται επιπρόσθετα σε χρηματική ικανοποίηση.

2. Η κατά το άρθρο 932 Α.Κ. χρηματική ικανοποίηση λόγω ηθικής βλάβης για παράβαση των υποχρεώσεων των παρόχων υπηρεσιών εμπιστοσύνης ορίζεται, κατ' ελάχιστο, στο ποσό των πέντε χιλιάδων ευρώ (5.000 €), εκτός αν ζητηθεί από τον ενάγοντα μικρότερο ποσό.

3. Οι ΠΥΕ ευθύνονται οι ίδιοι για τις πράξεις και παραλείψεις τυχόν τρίτων εξουσιοδοτημένων προσώπων στα οποία έχουν αναθέσει την άσκηση για λογαριασμό τους των καθηκόντων των προβλεπόμενων στον Κανονισμό eIDAS, το ν.4727/2020, όπως ισχύει, και την παρούσα απόφαση.

Άρθρο 18

Εποπτεία

1. Η ΕΕΤΤ εποπτεύει τους ΠΥΕ για την εφαρμογή και τήρηση των διατάξεων του Κανονισμού 910/2014 (ΕΕ), του Ν. 4727/2020, καθώς και της παρούσας απόφασης.

2. Για την άσκηση των καθηκόντων της μπορεί να διενεργεί επιτόπιους ελέγχους στα γραφεία των ΠΥΕ και τρίτων συμβεβλημένων προσώπων.

3. Οι ΠΥΕ υποχρεούνται να διευκολύνουν την πρόσβαση σε κάθε αρχείο, έγγραφο κ.λπ. που τυχόν ζητηθεί από τα εντεταλμένα από την ΕΕΤΤ πρόσωπα για τους σκοπούς του ελέγχου. Επίσης, υποχρεούνται να παρέχουν κάθε πληροφορία που ζητείται από την ΕΕΤΤ και να διευκολύνουν με κάθε δυνατό τρόπο το έργο της.

Με σχόλια [SP2]: 1.Προτείνουμε την απαλοιφή της διάταξης σχετικά με την επιβολή χρηματικής ικανοποίησης λόγω ηθικής βλάβης. Η υποχρέωση για αποζημίωση λόγω ηθικής βλάβης σημαίνει ότι οι ΠΥΕ έχουν προκαλέσει ζημία στον αντισυμβαλλόμενό τους με πράξη ή παράλειψη η οποία είναι παράνομη και υπαίτια. Κάτι τέτοιο όμως δεν θα πρέπει να προβλέπεται επειδή οι παρεχόμενες από τους ΠΥΕ υπηρεσίες προβλέπονται μέσα από τις συμβατικές τους υποχρεώσεις με κάθε αντισυμβαλλόμενό τους. Επομένως πρόκειται πάντοτε για συμβατικές υποχρεώσεις που πιθανώς δεν θα έχουν εκπληρωθεί. Επομένως κάθε πιθανή παράβαση των όρων της σύμβασης δεν μπορεί να οδηγεί σε αδικοπραξία.
2.Επιπρόσθετα στο άρθρο 13 της οδηγίας 910/2014 προβλέπεται η υποχρέωση αποζημίωσης για ζημία που προκαλείται από μη συμμόρφωση στις διατάξεις του κανονισμού. Οι ΠΥΕ έχουν τη δυνατότητα να θέσουν περιορισμούς στη χρήση των υπηρεσιών που παρέχουν και να μη φέρουν ευθύνη για ζημίες που προκύπτουν από χρήση υπηρεσιών υπερβαίνουσα αυτούς τους περιορισμούς. Η ενημέρωση των πελατών αποτελεί απαράβατο σχετικό όρο. Επομένως η ενημέρωση των πελατών για τους όρους παροχής των υπηρεσιών αυτομάτως καταργεί την ύπαρξη αδικοπραξίας και της εξ αυτής αποζημίωσης.
3.Επίσης σε κάθε περίπτωση η επιβολή ελάχιστου ορίου 5.000 ευρώ αποτελεί υπέρμετρα αυστηρά όριο και θα αυξήσει τόσο το κόστος των παρεχόμενων υπηρεσιών όσο και τα έξοδα στα οποία θα πρέπει να υποβληθούν οι ΠΥΕ για την ασφαλιστική τους κάλυψη.
4.Για τους λόγους αυτούς προτείνουμε αφενός την εξάλειψη του όρου για αναγνώριση αποζημίωσης λόγω ηθικής βλάβης και σε περίπτωση που τα ανωτέρω δεν γίνουν αποδεκτά τον περιορισμό του ορίου στα 1.000 ευρώ.

Παράρτημα 1

Αναφορά εκτίμησης κινδύνων και μέτρων αντιμετώπισης των περιστατικών ασφάλειας

Η αναφορά εκτίμησης κινδύνων θα πρέπει τουλάχιστον να περιλαμβάνει:

Α. Μεθοδολογία διαχείρισης κινδύνων

1. Προσδιορισμός στοιχείων που μπορεί να επηρεαστούν από ένα συμβάν, όπως: πλατφόρμα Αρχής Πιστοποίησης (CA), πλατφόρμα Αρχής Επικύρωσης (Validation Authority - VA), πλατφόρμα Αρχής Χρονοσφραγίδας (Timestamping Authority - TSA), Πλατφόρμα Αρχής Εγγραφής (Registration Authority - RA), πλατφόρμα δημιουργίας και επικύρωσης υπογραφών / σφραγίδων, πλατφόρμα διατήρησης υπογραφών / σφραγίδων, πλατφόρμα υπηρεσίας συστημένης παράδοσης, πλατφόρμα δικτύου, αρχείο, υλικό, λογισμικό αλλά και περιουσιακά στοιχεία, φήμη κ.λπ.
2. Προσδιορισμός των αιτίων που μπορεί να προκαλέσουν ένα συμβάν και τα οποία εντάσσονται στις εξής κύριες κατηγορίες: ανθρώπινο λάθος, κακόβουλες ενέργειες, φυσικές καταστροφές, αποτυχία συστήματος, αποτυχία τρίτων μερών.
3. Ανάλυση των ευπαθειών:
    i. κατά τη διαδικασία εγγραφής: εγγραφή θέματος, εξουσιοδότηση, αρχείο εγγραφής,
    ii. κατά τη διαδικασία διαχείρισης κλειδιού του ΠΥΕ: δημιουργία ζευγών κλειδιών, αποθήκευση ζευγών κλειδιών, δημιουργία αντιγράφων ασφαλείας και ανάκτηση,
    iii. κατά τη διαδικασία διαχείρισης κλειδιού του συνδρομητή: δημιουργία του ζεύγους κλειδιών,
    iv. κατά τη διαδικασία δημιουργίας πιστοποιητικού: παράδοση στο χρήστη, εγκατάσταση στην ΕΔΔΥ,
    v. κατά τη διαδικασία διαχείρισης ανάκλησης: διαδικασία διαχείρισης ανάκλησης πιστοποιητικού, δημοσιοποίηση της κατάστασης ανάκλησης πιστοποιητικού,
    vi. κατά τη διαδικασία επικύρωσης πιστοποιητικού, εφόσον παρέχεται, vii. κατά τη διαδικασία δημιουργίας χρονοσφραγίδας, εφόσον παρέχεται, viii. κατά την εγκατάσταση, ενημέρωση και χρήση των συστημάτων πληροφορικής και των δικτύων επικοινωνιών στα οποία βασίζεται η λειτουργία των υπηρεσιών του ΠΥΕ,
    ix. ό,τι άλλο επηρεάζει τον ΠΥΕ: πολιτικές, επιχειρησιακές διαδικασίες, προσωπικό, εγκαταστάσεις.
4. Προσδιορισμός των αναγκαίων / απαιτούμενων ελέγχων και μέτρα ασφαλείας:
    i. κατά τη διαδικασία εγγραφής.
    ii. κατά τη διαδικασία διαχείρισης κλειδιού του ΠΥΕ.
    iii. iii. κατά τη διαδικασία διαχείρισης κλειδιού του συνδρομητή,
    iv. κατά τη διαδικασία δημιουργίας του πιστοποιητικού,
    v. κατά τη διαδικασία διαχείρισης ανάκλησης,

vi. κατά τη διαδικασία επικύρωσης πιστοποιητικού, εφόσον παρέχεται,

vii. κατά τη διαδικασία δημιουργίας χρονοσφραγίδας, εφόσον παρέχεται,

viii. κατά την εγκατάσταση, ενημέρωση και χρήση των συστημάτων πληροφορικής και των δικτύων επικοινωνιών στα οποία βασίζεται η λειτουργία των υπηρεσιών του ΠΥΕ,

ix. στις λειτουργίες του ΠΥΕ: πολιτικές, επιχειρησιακές διαδικασίες, προσωπικό, εγκαταστάσεις.

5. Προσδιορισμός των συνεπειών: ενδεικτικά, παράνομη έκδοση πιστοποιητικών, δόλια χρήση έγκυρων πιστοποιητικών, δόλια χρήση ανακληθέντων πιστοποιητικών, αδυναμία έκδοσης πιστοποιητικών, αδυναμία χρήσης έγκυρων πιστοποιητικών, αδυναμία ανάκλησης πιστοποιητικών, απόρριψη πιστοποιητικού, ευθύνη, απώλεια φήμης, απώλεια κατάστασης πιστοποίησης.
6. Ανάλυση κινδύνων
    i. Αξιολόγηση του αντίκτυπου: Ο αντίκτυπος ορίζεται ως το αποτέλεσμα του ανεπιθύμητου περιστατικού. Μπορεί να μετρηθεί από τις συνέπειες που έχει το περιστατικό στον ΠΥΕ.

    ii. Αξιολόγηση της πιθανότητας.

    iii. Εκτίμηση του βαθμού κινδύνου.
7. Εκτίμηση κινδύνων
    i. Περιγραφή: Συνοπτική περιγραφή των χαρακτηριστικών του προσδιορισμένου κινδύνου και της πιθανότητας και του βαθμού επίδρασης

    ii. Σχετικά περιουσιακά στοιχεία

    iii. Πιθανές ευπάθειες

    iv. Πιθανές απειλές

    v. Πιθανές συνέπειες

Β. Γενική διαδικασία περιορισμού περιστατικών

1. Ετοιμότητα: ενεργοποίηση μέσων για τη συλλογή ειδοποιήσεων, ενεργοποίηση ειδοποιήσεων στα εσωτερικά συστήματα, συνεχής αυτο-παρακολούθηση και αυτοέλεγχος, δημιουργία δυνατότητας αντιμετώπισης περιστατικών, προετοιμασία προσωπικού και συστημάτων για ένα περιστατικό, δημιουργία καναλιών επικοινωνίας με όλους τους ενδιαφερόμενους, δημιουργία χώρου αποθήκευσης πληροφοριών επαφών με τους κατόχους πιστοποιητικών, δημιουργία αποθετηρίου εποπτικών αρχών και αρμόδιων αρχών, σχέδια αντιμετώπισης έκτακτης ανάγκης, ενημερωμένες πληροφορίες για το περιβάλλον.
2. Εντοπισμός και αξιολόγηση του συμβάντος: δραστηριότητες παράνομης πιστοποίησης, μη φυσιολογικές δραστηριότητες σε συστήματα πληροφοριών, ύποπτες πληροφορίες στα αρχεία καταγραφής διαχείρισης κύκλου ζωής πιστοποιητικών, μη αναγνωρισμένα κλειδιά, απώλεια διαθεσιμότητας, απώλεια κυριότητας κλειδιού.

3. Απόκριση στο περιστατικό: καταγραφή τύπων παραβίασης, πλάνο απόκρισης αναλόγως της παραβίασης.
4. Εξάλειψη /επίλυση του περιστατικού: καθορισμός των συνθηκών που ευνοούν το περιστατικό, ανάλυση των πολιτικών και διαδικασιών ασφάλειας, επαναξιολόγηση κινδύνου, καθορισμός και εφαρμογή διορθωτικών μέτρων.

Παράρτημα 2

Αίτηση Έναρξης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης

<table>
<tr><td colspan="3">ΜΕΡΟΣ Α – ΣΤΟΙΧΕΙΑ ΑΙΤΟΥΝΤΑ</td></tr>
<tr><td colspan="2">ΔΙΑΚΡΙΤΙΚΟΣ ΤΙΤΛΟΣ / ΕΠΩΝΥΜΙΑ
(Όπως εμφανίζεται στην επίσημη καταχώρηση)</td><td>ΝΟΜΙΚΗ ΜΟΡΦΗ</td></tr>
<tr><td colspan="2">ΝΟΜΙΜΟΙ ΕΚΠΡΟΣΩΠΟΙ :
1.
2.
3.
4.
5.</td><td>ΑΝΤΙΚΛΗΤΟΣ :</td></tr>
<tr><td>ΑΦΜ :</td><td>ΔΟΥ :</td><td>Αριθμός Γ.Ε.ΜΗ. :</td></tr>
<tr><td colspan="3">Διεύθυνση Έδρας:</td></tr>
<tr><td colspan="3">ΠΟΛΗ / Ταχ. ΚΩΔΙΚΟΣ :</td></tr>
<tr><td colspan="3">ΧΩΡΑ :</td></tr>
<tr><td colspan="3">ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΜΕ ΤΟ ΚΟΙΝΟ
ΤΗΛΕΦΩΝΟ : FAX : Email</td></tr>
<tr><td colspan="3">Ιστοσελίδα:</td></tr>
<tr><td colspan="3">ΕΚΠΡΟΣΩΠΟΙ ΕΠΙΚΟΙΝΩΝΙΑΣ ΜΕ ΤΗΝ ΕΕΤΤ Email
ΟΝΟΜΑΤΕΠΩΝΥΜΟ : ΤΗΛΕΦΩΝΟ:
1.
2.
3.</td></tr>
</table>

ΜΕΡΟΣ Β – ΥΠΗΡΕΣΙΕΣ ΕΜΠΙΣΤΟΣΥΝΗΣ ΓΙΑ ΤΙΣ ΟΠΟΙΕΣ ΖΗΤΕΙΤΑΙ Η ΕΓΚΡΙΣΗ ΤΗΣ ΕΕΤΤ
☐ Δημιουργία εγκεκριμένης Ηλεκτρονικής Υπογραφής (άρθρο 28 του Κανονισμού eIDAS)
☐ Δημιουργία εγκεκριμένης Ηλεκτρονικής Σφραγίδας (άρθρο 38 του Κανονισμού eIDAS)
☐ Επικύρωση εγκεκριμένης Ηλεκτρονικής Υπογραφής (άρθρο 33 του Κανονισμού eIDAS)
☐ Επικύρωση εγκεκριμένης Ηλεκτρονικής Σφραγίδας (άρθρο 40 του Κανονισμού eIDAS)
☐ Διαφύλαξη εγκεκριμένης Ηλεκτρονικής Υπογραφής (άρθρο 34 του Κανονισμού eIDAS)
☐ Διαφύλαξη εγκεκριμένης Ηλεκτρονικής Σφραγίδας (άρθρο 40 του Κανονισμού eIDAS)
☐ Δημιουργία εγκεκριμένης Ηλεκτρονικής Χρονοσφραγίδας (άρθρο 42 του Κανονισμού eIDAS)
☐ Εγκεκριμένη Υπηρεσία Συστημένης Παράδοσης (άρθρο 44 του Κανονισμού eIDAS)
☐ Δημιουργία, εξακρίβωση και επικύρωση εγκεκριμένων πιστοποιητικών για επαλήθευση της ταυτότητας ιστοτόπων (άρθρο 45 του Κανονισμού eIDAS)

ΜΕΡΟΣ Γ – ΟΙΚΟΝΟΜΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ
Στοιχεία σχετικά με τους οικονομικούς πόρους του Παρόχου επισυνάπτονται[1].
Οι οικονομικοί πόροι προέρχονται από:
☐ Κεφαλαιακή επάρκεια (Ίδια κεφάλαια)
☐ Ασφαλιστικές καλύψεις
☐ Όλα τα ανωτέρω
☐ Άλλο

ΜΕΡΟΣ Δ – ΕΞΑΝΤΛΗΤΙΚΟΣ ΚΑΤΑΛΟΓΟΣ ΤΩΝ ΕΠΙΣΥΝΑΠΤΟΜΕΝΩΝ ΕΓΓΡΑΦΩΝ

[1] Οι εσωκλειόμενες πληροφορίες πρέπει να αποδεικνύουν επαρκείς οικονομικούς πόρους για να ανταπεξέλθει η εταιρεία στις από το νόμο υποχρεώσεις της.

☐	Έκθεση Αξιολόγησης της Συμμόρφωσης (ΕΑΣ)
☐	Πιστοποιητικό εγγραφής στο Γενικό Εμπορικό Μητρώο (Γ.Ε.ΜΗ.)
☐	Πιστοποιητικό/ βεβαίωση του οικείου επαγγελματικού ή εμπορικού μητρώου για την εγγραφή του σε αυτό. Εφόσον πρόκειται για νομικό πρόσωπο, πιστοποιητικό/ βεβαίωση εμπορικού επιμελητηρίου ή άλλης αντίστοιχης αρμόδιας δημόσιας υπηρεσίας
☐	Πιστοποιητικό ασφαλιστικής ενημερότητας
☐	Πιστοποιητικό φορολογικής ενημερότητας
☐	Ενιαίο Πιστοποιητικό Δικαστικής Φερεγγυότητας από το αρμόδιο Πρωτοδικείο, από το οποίο προκύπτει ότι δεν τελούν υπό πτώχευση, πτωχευτικό συμβιβασμό ή υπό αναγκαστική διαχείριση ή δικαστική εκκαθάριση ή ότι δεν έχουν υπαχθεί σε διαδικασία εξυγίανσης
☐	Εκτύπωση της καρτέλας «Στοιχεία Μητρώου/Επιχείρησης» από την ηλεκτρονική πλατφόρμα της Ανεξάρτητης Αρχής Δημοσίων Εσόδων, όπως αυτά εμφανίζονται στο Taxisnet, από την οποία να προκύπτει η μη αναστολή της επιχειρηματικής δραστηριότητάς τους
☐	Ισολογισμούς τουλάχιστον των τριών (3) τελευταίων ετών, που έχουν ολοκληρωθεί, εφόσον δημοσιεύονται, ή υπεύθυνη δήλωση του Ν. 1599/1986 του συνολικού ύψους του ετήσιου κύκλου εργασιών τα δύο (2) τελευταία χρόνια, σε περίπτωση που δεν υπάρχει υποχρέωση δημοσίευσης. Εφόσον ο αιτών δραστηριοποιείται για μικρότερο χρονικό διάστημα, υποβάλλει αποσπάσματα οικονομικών καταστάσεων ή δήλωση για το εν λόγω χρονικό διάστημα
☐	Πολιτική Υπηρεσίας Εμπιστοσύνης (Trust Service Policy) και Δήλωση Πρακτικής (Trust Service Practice Statement) για κάθε υπηρεσία που ζητείται η έγκριση, συνοδευόμενα από ένα ενεργό και έγκυρο URL, όπου είναι δημοσιευμένα τα εν λόγω έγγραφα (URL:)
☐	Πιστοποιητικά των Αρχών Πιστοποίησης που θα χρησιμοποιηθούν για την παροχή της υπηρεσίας και δείγματα (Test samples) των πιστοποιητικών ή άλλων στοιχείων που θα εκδοθούν ή θα δημιουργηθούν στο πλαίσιο κάθε υπό έγκριση υπηρεσίας
☐	Αναφορά αποτίμησης κινδύνου
☐	Σχέδιο Ειδοποίησης του τελικού χρήστη, σε περίπτωση συμβάντος ασφαλείας
☐	Σχέδιο Τερματισμού λειτουργίας
☐	Αντίγραφο της τυποποιημένης Σύμβασης με τους τελικούς χρήστες που περιλαμβάνει τους Όρους Χρήσης της υπηρεσίας

ΜΕΡΟΣ Ε – ΥΠΟΓΡΑΦΗ

Ο παρακάτω υπογράφων αιτούμαι την εγγραφή της εταιρείας που εκπροσωπώ στο αρχείο ΠΥΕ που τηρεί η ΕΕΤΤ και την έγκριση της ΕΕΤΤ για την παροχή των υπηρεσιών που περιλαμβάνονται στην αίτηση και δηλώνω ότι όλες οι παρεχόμενες πληροφορίες είναι ορθές.

Ημερομηνία: Τόπος:

Υπογραφή Νόμιμου Εκπροσώπου

Παράρτημα 3

Προτεινόμενος πίνακας περιεχομένων για το Σχέδιο Τερματισμού

1. Αρχική σελίδα

(I) Όνομα εγγράφου και ταυτότητα, συμπεριλαμβανομένων των εξής: Αριθμός Έκδοσης, Ημερομηνία Έναρξης Ισχύος, Κατάσταση και Ταξινόμηση εγγράφων.

(Ii) Ταυτοποίηση του εγκεκριμένου ΠΥΕ: Σαφής προσδιορισμός του ονόματος του ΠΥΕ και, κατά περίπτωση, του αριθμού εγγραφής, όπως αναφέρεται στα επίσημα αρχεία, της επίσημης ταχυδρομικής διεύθυνσης και της διεύθυνσης ηλεκτρονικού ταχυδρομείου.

(Iii) Ταυτοποίηση της σχετικής εγκεκριμένης υπηρεσίας εμπιστοσύνης.

2. Εισαγωγή

Αυτή η παράγραφος προσδιορίζει και εισάγει το σύνολο των προβλέψεων και υποδεικνύει τις εγκεκριμένες υπηρεσίες εμπιστοσύνης που αφορά το σχέδιο τερματισμού.

2.1. Επισκόπηση

Αυτή η παράγραφος παρέχει μια γενική επισκόπηση του σχεδίου τερματισμού και μια σύνοψη των εγκεκριμένων υπηρεσιών εμπιστοσύνης που αφορούν οι διατάξεις του σχεδίου τερματισμού. Ανάλογα με την πολυπλοκότητα και το εύρος της εγκεκριμένης υπηρεσίας μπορεί να είναι χρήσιμη μια διαγραμματική αναπαράσταση. Όλοι οι συμμετέχοντες και τα στοιχεία κάθε εγκεκριμένης υπηρεσίας πρέπει να προσδιορίζονται επαρκώς.

2.2. Όνομα εγγράφου και κανόνες ταυτοποίησης

Αυτή η παράγραφος παρέχει τυχόν ισχύοντα ονόματα ή άλλα αναγνωριστικά στοιχεία για το έγγραφο του σχεδίου τερματισμού και για τα σχετικά έγγραφα αναφοράς, κατά περίπτωση.

2.3. Εγκεκριμένες υπηρεσίες για τις οποίες ισχύει το σχέδιο τερματισμού

Αυτή η παράγραφος παρέχει λεπτομερή καταγραφή των εγκεκριμένων υπηρεσιών για τις οποίες ισχύουν οι προβλέψεις του σχεδίου τερματισμού, ιδίως, όσον αφορά στις αντίστοιχες καταχωρίσεις στον Κατάλογο Υπηρεσιών Εμπιστοσύνης και τα σχετικά με αυτές αναγνωριστικά τύπου υπηρεσίας (service type identifiers). Εξαρτάται από την πολυπλοκότητα και το εύρος της παροχής υπηρεσίας, το αν θα είναι χρήσιμη μια διαγραμματική απεικόνιση ή ένας πίνακας.

2.4. Διαχείριση σχεδίου τερματισμού

Αυτή η παράγραφος περιλαμβάνει το όνομα και τη διεύθυνση επικοινωνίας του οργανισμού ή της αρχής που είναι υπεύθυνη για τη σύνταξη, καταχώριση, διατήρηση και ενημέρωση του σχεδίου τερματισμού. Επίσης προσδιορίζει τις ευθύνες και τα καθήκοντα του εν λόγω οργανισμού ή αρχής, όσον αφορά στον τερματισμό του ΠΥΕ/ μιας εγκεκριμένης υπηρεσίας εμπιστοσύνης, στην αναθεώρηση του σχεδίου τερματισμού, στις δοκιμές και στις διαδικασίες ελέγχου, και στην εκτέλεσή της. Η παράγραφος περιλαμβάνει επίσης το όνομα, τη διεύθυνση ηλεκτρονικού

ταχυδρομείου, τον αριθμό τηλεφώνου και τον αριθμό φαξ του υπευθύνου επικοινωνίας, τη θέση του ή το λειτουργικό του ρόλο.

2.5. Εφαρμοστέα εθνική νομοθεσία και σχετικές διατάξεις που διέπουν τον τερματισμό εργασιών του ΠΥΕ ή μίας εγκεκριμένης υπηρεσίας εμπιστοσύνης

Αυτή η παράγραφος παρέχει αναφορές στην ισχύουσα εθνική νομοθεσία και προσδιορίζει τις σχετικές διατάξεις που διέπουν τον τερματισμό των εργασιών του ΠΥΕ ή μίας εγκεκριμένης υπηρεσίας εμπιστοσύνης.

3. Διατάξεις σχετικές με τον τερματισμό

3.1. Προγραμματισμένος τερματισμός

Ο προγραμματισμένος τερματισμός μπορεί να συμβεί στις εξής περιπτώσεις:

- Στο πλαίσιο των ενεργειών προγραμματισμένου τερματισμού μέρους ή του συνόλου μιας εγκεκριμένης υπηρεσίας, στην οποία εφαρμόζεται το σχέδιο τερματισμού ή
- Στο πλαίσιο προγραμματισμένων ενεργειών που δύνανται να οδηγήσουν σε μερική ή πλήρη διακοπή παροχής μιας εγκεκριμένης υπηρεσίας, στην οποία εφαρμόζεται το σχέδιο τερματισμού.

Οι σχετικές ενέργειες και οι συναφείς διατάξεις πρέπει να περιλαμβάνουν:

- Επικαιροποίηση του σχεδίου τερματισμού και των διατάξεων σχετικά με την κοινοποίησή του στον αρμόδιο Εποπτεύοντα Φορέα (ΕΕΤΤ).
- Καταγραφή των λειτουργιών που πρόκειται να παύσουν, του αναμενόμενου χρονοδιαγράμματος και του σχετικού προγραμματισμού των ενεργειών.
- Προσδιορισμός του αναμενόμενου αντίκτυπου στις σχετικές καταχωρίσεις του Καταλόγου Υπηρεσιών Εμπιστοσύνης.
- Επικαιροποίηση της ανάλυσης κινδύνου και επικαιροποιημένα μέτρα μετριασμού των κινδύνων.
- Εκτίμηση των οικονομικών πόρων ή της ασφαλιστικής κάλυψης που απαιτείται για την κάλυψη των εξόδων / επισφαλειών που σχετίζονται με τον τερματισμό των εργασιών ή μιας εγκεκριμένης υπηρεσίας.
- Επικαιροποίηση της εκτίμησης των επιπτώσεων για τα δεδομένα προσωπικού χαρακτήρα και επικαιροποιημένα μέτρα μετριασμού των.
- Ειδοποιήσεις τερματισμού.
    - Καταγραφή όλων των τρίτων μερών που πρέπει να ενημερωθούν για τον τερματισμό (ενδεικτικά: ΕΕΤΤ, συνδρομητές, κ.λπ.)
    - Για κάθε μέρος που πρέπει να ενημερωθεί για τον τερματισμό, καταγραφή του περιεχομένου της ενημέρωσης, του μέσου που πρόκειται να χρησιμοποιηθεί για την ενημέρωση και το σχετικό προγραμματισμό αποστολής των ειδοποιήσεων
    - Προετοιμασία σχετικού υλικού για τις ανωτέρω ειδοποιήσεις
        - Καταγραφή των εγκεκριμένων υπηρεσιών που έχει αποφασιστεί ο τερματισμός, του λόγου τερματισμού και του σχετικού χρονοδιαγράμματος
        - Όροι και προϋποθέσεις που διέπουν τη σχετική ενημέρωση, όπως:
- Διακανονισμός (-οι) που ισχύουν με ένα άλλο εγκεκριμένο ΠΥΕ για την παροχή μελλοντικών εγκεκριμένων υπηρεσιών εμπιστοσύνης παρόμοιας φύσης.
- Διατήρηση των σχετικών (προσωπικών) δεδομένων του συνδρομητή.

- Διατήρηση λειτουργικών δεδομένων και άλλων σχετικών δεδομένων για τη προστασία της αξιοπιστίας των πιστοποιητικών εγκεκριμένων υπηρεσιών εμπιστοσύνης και των σχετικών αποδεικτικών στοιχείων.
- Ενημέρωση σχετικά με τη διατήρηση σε ισχύ όσων εγκεκριμένων πιστοποιητικών της υπό τερματισμό εγκεκριμένης υπηρεσίας δεν έχουν λήξει ή την ανάκλησή τους • Προβλεπόμενες αποζημιώσεις στους συνδρομητές, κατά περίπτωση.
- Διαδικασίες εκτέλεσης ενεργειών τερματισμού • Καταγραφή του προσωπικού (του ΠΥΕ ή/και υπεργολάβων του) που εμπλέκεται στις διαδικασίες τερματισμού και της εμπειρίας του
- Ταυτοποίηση του φορέα (ΕΕΤΤ ή άλλος εγκεκριμένος ΠΥΕ), που αναλαμβάνει την τήρηση του αρχείου του ΠΥΕ

3.2. Μη προγραμματισμένος τερματισμός

Ο απροσδόκητος ή μη προγραμματισμένος τερματισμός του Παρόχου ή της υπηρεσίας μπορεί να οφείλεται σε διαφορετικές αιτίες όπως σοβαρό περιστατικό ή καταστροφή μετά από την οποία θα μπορούσε να επιτευχθεί μόνο ελλιπής ή μη ικανοποιητική ανάκτηση, πτώχευση, δικαστικές εντολές και τυχόν μη αναμενόμενο λόγο που αναγκάζει ο ΠΥΕ να εκτελέσει ένα τερματισμό.

Αυτή η παράγραφος περιγράφει τα μέτρα και τις δράσεις που πρέπει να αναληφθούν στο πλαίσιο του μη προγραμματισμένου τερματισμού μέρους ή του συνόλου της υπηρεσίας για την οποία εφαρμόζεται το εν λόγω σχέδιο τερματισμού, λαμβάνοντας υπόψη την απροσδόκητη και μη προγραμματισμένη φύση των αιτίων που προκάλεσαν τον τερματισμό και δυνητικά περιορισμένο χρονικό διάστημα εντός του οποίου πρέπει να αναληφθούν οι σχετικές αυτές δράσεις. Στην παράγραφο αυτή πρέπει να καταγράφονται οι ρόλοι και το πεδίο δράσης των πιθανών μεσαζόντων, ασφαλιστών ή τρίτων μερών.

4. Δοκιμές συμμόρφωσης, έλεγχος και άλλη αξιολόγηση

Αυτή η παράγραφος διευκρινίζει:

- Τον κατάλογο των στόχων που καλύπτονται από τη δοκιμή του σχεδίου τερματισμού ή / και τη μεθοδολογία δοκιμής που χρησιμοποιήθηκε για τη διεξαγωγή των δοκιμών.
- Τη συχνότητα των δοκιμών συμμόρφωσης ή άλλης αξιολόγησης.
- Την ταυτότητα ή / και τα προσόντα του προσωπικού που εκτελεί τον έλεγχο ή τη δοκιμή τερματισμού.
- Τη σχέση μεταξύ του προσωπικού δοκιμών και του εγκεκριμένου ΠΥΕ του οποίου το σχέδιο τερματισμού βρίσκεται υπό δοκιμή, συμπεριλαμβανομένου του βαθμού ανεξαρτησίας του προσωπικού δοκιμών.
- Τις δράσεις που λαμβάνονται ως αποτέλεσμα ελλείψεων που διαπιστώθηκαν κατά τη διάρκεια των δοκιμών του σχεδίου τερματισμού.
- Ποιος δικαιούται να δει τα αποτελέσματα των δοκιμών, ποιος τα παρέχει και πώς γνωστοποιούνται.

5. Άλλες διατάξεις

Αυτή η παράγραφος παρέχει οποιεσδήποτε άλλες εφαρμοστέες διατάξεις που δεν καλύπτονται στις ανωτέρω παραγράφους.