ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

ΚΕΙΜΕΝΟ ΔΗΜΟΣΙΑΣ ΔΙΑΒΟΥΛΕΥΣΗΣ ΑΝΑΦΟΡΙΚΑ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΕΜΠΙΣΤΟΣΥΝΗΣ

Μαρούσι, Οκτώβριος 2017

Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)

Πρόλογος

Το παρόν Κείμενο Δημόσιας Διαβούλευσης έχει ετοιμαστεί από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και αφορά τον νέο Κανονισμό για την παροχή υπηρεσιών εμπιστοσύνης, με τον οποίο ρυθμίζονται ζητήματα των υπηρεσιών εμπιστοσύνης που παρέχονται στην ελληνική επικράτεια, για την βέλτιστη εφαρμογή 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 ΕΕΤΤ προσκαλεί τους ενδιαφερόμενους φορείς να παρουσιάσουν τα σχόλια και τις απόψεις τους σχετικά με το προτεινόμενο σχέδιο Κανονισμού. 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 trustservices@eett.gr όχι αργότερα από την **25η Οκτωβρίου 2017** και ώρα 13:00. 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 φέρουν την ένδειξη:

Δημόσια Διαβούλευση Κανονισμού Παροχής Υπηρεσιών Εμπιστοσύνης

Οι απαντήσεις πρέπει να υποβάλλονται στην ακόλουθη διεύθυνση:

ΕΕΤΤ

Λ. Κηφισίας 60,

15125 Μαρούσι

Αττική

E-mail : trustservices@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: trustservices@eett.gr

Το παρόν κείμενο δεν δεσμεύει την ΕΕΤΤ ως προς το περιεχόμενο της ρύθμισης που θα επακολουθήσει.

1 Εισαγωγή

Η ΕΕΤΤ υποβάλλει σε Δημόσια Διαβούλευση, σύμφωνα με το άρθρο 17 του ν. 4070/2012 (ΦΕΚ 82 Α'), σχέδιο «Κανονισμού Παροχής Υπηρεσιών Εμπιστοσύνης», με τον οποίο ρυθμίζονται ζητήματα εφαρμογής, στην ελληνική έννομη τάξη, 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».

Στόχος της παρούσας Δημόσιας Διαβούλευσης είναι να λάβει η ΕΕΤΤ τις απόψεις και τα σχόλια όλων των ενδιαφερόμενων φορέων με σκοπό τη βέλτιστη ρύθμιση των υποχρεώσεων και των ειδικών διαδικασιών που αφορούν την παροχή των υπηρεσιών εμπιστοσύνης, εγκεκριμένων και μη.

2. Αιτιολογικές Σκέψεις

Την 1/7/2016 ετέθη σε ισχύ ο Κανονισμός (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 και την κατάργηση της Οδηγίας 1999/93/ΕΚ (Κανονισμός eIDAS). Με τον Κανονισμό αυτόν θεσπίζονται κανόνες για τις υπηρεσίες εμπιστοσύνης, ιδίως στις ηλεκτρονικές συναλλαγές και θεσπίζεται ενιαίο ευρωπαϊκό πλαίσιο για την παροχή και τη χρήση των υπηρεσιών και προϊόντων εμπιστοσύνης, στις οποίες περιλαμβάνονται οι ηλεκτρονικές υπογραφές, οι ηλεκτρονικές σφραγίδες, οι ηλεκτρονικές χρονοσφραγίδες, οι ηλεκτρονικές υπηρεσίες συστημένης παράδοσης και τα πιστοποιητικά επαλήθευσης της ταυτότητας ιστοτόπων.

Με σχόλια [DZ1]: Σύμφωνα με τον Κανονισμό, Άρθρο 3 ορισμός 16, ορίζονται συγκεκριμένες «Υπηρεσίες Εμπιστοσύνης»:
1.Δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών υπογραφών (e-Signatures)
2.Δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών σφραγίδων (e-Seals)
3.Δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών χρονοσφραγίδων (Time Stamping)
4.Δημιουργία, εξακρίβωση και επικύρωση πιστοποιητικών για επαλήθευση ταυτότητας ιστοτόπων (Web Site Authentication)
5.Ηλεκτρονικές υπηρεσίες συστημένης παράδοσης (e-Delivery)
6.Ηλεκτρονικές υπηρεσίες διαφύλαξης ηλεκτρονικών υπογραφών, σφραγίδων ή πιστοποιητικών (e-Preservation)
Προτείνεται να υιοθετηθεί ακριβώς η επίσημη μετάφραση στις ορολογίες του Κανονισμού. Δείτε και https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas στο ερώτημα "**In addition to eSignature, which other trust services fall under eIDAS?**"

Ο Κανονισμός eIDAS ορίζει ειδικότερες απαιτήσεις για τους παρόχους υπηρεσιών εμπιστοσύνης, όσον αφορά την ασφάλεια και την ευθύνη για τη διασφάλιση της δέουσας επιμέλειας, της διαφάνειας και της λογοδοσίας των δραστηριοτήτων και των υπηρεσιών τους. Διακρίνει δε μεταξύ εγκεκριμένων και μη εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης και θέτει ιδιαίτερες υποχρεώσεις για τους εγκεκριμένους παρόχους.

Για την βέλτιστη εφαρμογή του Κανονισμού eIDAS στην ελληνική έννομη τάξη θα πρέπει να θεσπιστεί ένα ειδικότερο κανονιστικό πλαίσιο για τη ρύθμιση ειδικότερων ζητημάτων, διαδικασιών και υποχρεώσεων των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών εμπιστοσύνης.

Η ΕΕΤΤ αποτελεί τον εθνικό εποπτικό φορέα με τα καθήκοντα του άρθρου 17 του Κανονισμού eIDAS. Ειδικότερα, σύμφωνα με το άρθρο 48 Ν. 4487/2017

(ΦΕΚ Α' 116), με το οποίο αντικαταστάθηκε η περίπτωση κε΄ του άρθρου 12 του Ν. 4070/2012, ορίζεται η αρμοδιότητα της ΕΕΤΤ να: «κε΄. Ρυθμίζει με αποφάσεις της τα ζητήματα των υπηρεσιών εμπιστοσύνης. Ασκεί τα καθήκοντα και τις αρμοδιότητες του εποπτικού φορέα υπηρεσιών εμπιστοσύνης, σύμφωνα με τα προβλεπόμενα στον Κανονισμό (ΕΕ) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 και ιδίως στο άρθρο 17 αυτού. Καταρτίζει, τηρεί και δημοσιεύει τον εθνικό κατάλογο εμπιστοσύνης, σύμφωνα με το άρθρο 22 του ίδιου Κανονισμού ΕΕ και ενημερώνει σχετικά την Ευρωπαϊκή Επιτροπή.»

Η ΕΕΤΤ θέτει σε δημόσια διαβούλευση τον παρόντα Κανονισμό Παροχής Υπηρεσιών Εμπιστοσύνης με τον οποίο ρυθμίζονται ιδίως τα κάτωθι ζητήματα:

- Οι γενικές υποχρεώσεις των παρόχων υπηρεσιών εμπιστοσύνης, εγκεκριμένων και μη.
- Τήρηση Αρχείου των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών εμπιστοσύνης
- Απαιτήσεις ασφάλειας για τους παρόχους υπηρεσιών εμπιστοσύνης
- Υποχρέωση αναφοράς συμβάντων στην ΕΕΤΤ
- Διαδικασίες έναρξης παροχής εγκεκριμένων υπηρεσιών εμπιστοσύνης
- Διαδικασίες τερματισμού εργασιών
- Υποχρέωση γνωστοποίησης τερματισμού εργασιών
- Υποχρέωση υποβολής Έκθεσης Αξιολόγησης Συμμόρφωσης
- Ανάκληση εγκεκριμένων πιστοποιητικών
- Τήρηση Αρχείου εγκεκριμένων πιστοποιητικών

Με σχόλια [DZ2]: Καλό θα ήταν να υπάρξει μέριμνα για τις περιπτώσεις απομακρυσμένης υπογραφής, ιδιαίτερα όταν αυτές οι υπηρεσίες παρέχονται από συνεργαζόμενους φορείς με τον Πάροχο και όχι από τον ίδιο τον Πάροχο.

Με σχόλια [DZ3]: Το Αρχείο θα πρέπει να αφορά όχι μόνο τα εγκεκριμένα πιστοποιητικά αλλά όλες τις υπηρεσίες που περιγράφονται στον Κανονισμό eIDAS.

Ακολούθως παρατίθεται το Σχέδιο του Κανονισμού:

«ΚΑΝΟΝΙΣΜΟΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΕΜΠΙΣΤΟΣΥΝΗΣ»

Μέρος Α: Γενικές Διατάξεις

Άρθρο 1
Σκοπός και πεδίο εφαρμογής του Κανονισμού

1.1. Σκοπός του παρόντος Κανονισμού είναι η ρύθμιση ζητημάτων των υπηρεσιών εμπιστοσύνης και των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών εμπιστοσύνης σε συμπλήρωση του Κανονισμού (ΕΕ) αρ. 910/2014 eIDAS.

1.2. Οι διατάξεις του παρόντος δεν θίγουν διατάξεις που, αναφορικά με τη σύναψη και την ισχύ συμβάσεων ή εν γένει τη σύσταση νομικών υποχρεώσεων, επιβάλλουν τη χρήση συγκεκριμένου τύπου, ούτε διατάξεις για την αποδεικτική ή άλλη χρήση εγγράφων ή διατάξεις με τις οποίες απαγορεύεται να διακινούνται και να καθίστανται γνωστά έγγραφα ορισμένων κατηγοριών και δεδομένα προσωπικού χαρακτήρα.

Άρθρο 2
Ορισμοί και Ακρωνύμια

2.1 Για την εφαρμογή του παρόντος Κανονισμού ισχύουν οι ακόλουθοι ορισμοί:

Υπηρεσίες εμπιστοσύνης: είναι οι ηλεκτρονικές υπηρεσίες, που παρέχονται κατά κανόνα έναντι αμοιβής και έχουν ως αντικείμενο τη δημιουργία, εξακρίβωση, επικύρωση και διαφύλαξη ηλεκτρονικών υπογραφών, ηλεκτρονικών σφραγίδων, ηλεκτρονικών χρονοσφραγίδων, ηλεκτρονικών υπηρεσιών συστημένης παράδοσης και πιστοποιητικών που σχετίζονται με αυτές τις υπηρεσίες, καθώς και στη δημιουργία, εξακρίβωση και διατήρηση πιστοποιητικών για επαλήθευση της ταυτότητας ιστοτόπων, εφόσον εμπίπτουν στο πεδίο εφαρμογής του Κανονισμού eIDAS.

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

Εθνικός Κατάλογος Εμπιστοσύνης (National Trust List - NTL): Ο κατάλογος εμπιστοσύνης συμπεριλαμβανομένων των πληροφοριών σχετικά με τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης εγκατεστημένους στην Ελλάδα, καθώς και πληροφορίες σχετικά με τις εγκεκριμένες υπηρεσίες εμπιστοσύνης που αυτοί παρέχουν. Τον Εθνικό Κατάλογο 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.

Με σχόλια [DZ4]: Προτείνεται να γίνει απευθείας παραπομπή ή αντιγραφή του Άρθρου 3, ορισμός 16 και 17 (βλ. προηγούμενο σχόλιο). Αν πρέπει να αναλυθούν όλες οι υπο-περιπτώσεις (πχ να εμφανίζονται ξεχωριστά οι υπηρεσίες:
1.Δημιουργία ηλ. Υπογραφών (creation) άρθρο 28
2.Επικύρωση ηλ. Υπογραφών (validation) Άρθρα 32, 33
3.Διαφύλαξη ηλ. Υπογραφών (preservation) Άρθρο 34
4.Δημιουργία ηλ. Σφραγίδων (creation) άρθρο 38
5.Επικύρωση και διαφύλαξη ηλ. Σφραγίδων (validation and preservation) Άρθρο 40 (τα έχει μαζί για τις σφραγίδες)
6.Ηλεκτρονική Χρονοσφραγίδα Άρθρο 42
7.Συστημένη Παράδοση, άρθρο 43
8.Πιστοποίηση γνησιότητας ιστοτόπων, άρθρο 45)

θα υπάρχει σύγχυση σε σχέση με την ομαδοποίηση που υπάρχει στο άρθρο 3, ορισμός 16. Οι περισσότεροι φορείς εξωτερικής αξιολόγησης, χρησιμοποιούν την ομαδοποίηση του άρθρου 3.

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

2.3 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)

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

Άρθρο 3
Τήρηση Αρχείου των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών εμπιστοσύνης

3.1. Η ΕΕΤΤ τηρεί ηλεκτρονικό αρχείο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Εμπιστοσύνης, εγκεκριμένων και μη, σε ηλεκτρονική ή/και έντυπη μορφή.

3.2. Κάθε εγκατεστημένος στην Ελλάδα Πάροχος Υπηρεσιών Εμπιστοσύνης γνωστοποιεί με αίτησή του ηλεκτρονικά στην ΕΕΤΤ τα ακόλουθα στοιχεία, τα οποία καταχωρούνται στο ηλεκτρονικό αρχείο της ΕΕΤΤ:
   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 (Παράρτημα 1: Παρεχόμενες εγκεκριμένες υπηρεσίες, Παράρτημα 2: Παρεχόμενες μη εγκεκριμένες υπηρεσίες)

3.3. Κάθε Πάροχος Υπηρεσιών Εμπιστοσύνης που παρέχει Εγκεκριμένα Πιστοποιητικά ηλεκτρονικής υπογραφής ή Εγκεκριμένες ηλεκτρονικές σφραγίδες, εκτός από τα στοιχεία του σημείου 2 ανωτέρω, υποβάλλει όσα προβλέπονται στο Άρθρο 6 περί έναρξης εργασιών.

Με σχόλια [DZ5]: Κανονισμός, Άρθρο 3 ορισμός 15

Με σχόλια [DZ6]: Κανονισμός, Άρθρο 3 ορισμός 27

Με σχόλια [DZ7]: Προτείνεται να αντικατασταθεί από «Εγκεκριμένες Υπηρεσίες Εμπιστοσύνης»

3.4. Για την καταχώρηση των ανωτέρω στοιχείων στο ηλεκτρονικό αρχείο της ΕΕΤΤ, επιβάλλεται τέλος καταχώρησης, ύψους € 300 (τριακοσίων ευρώ), το οποίο καταβάλλεται με την υποβολή της αίτησης.

3.5. Οι Πάροχοι Υπηρεσιών Εμπιστοσύνης υποχρεούνται να γνωστοποιούν ηλεκτρονικά στην ΕΕΤΤ κάθε τροποποίηση των στοιχείων τους που περιλαμβάνονται στο ηλεκτρονικό αρχείο της ΕΕΤΤ εντός αποκλειστικής προθεσμίας επτά (7) ημερών από την επέλευσή της.
3.6. Οι Πάροχοι Υπηρεσιών Εμπιστοσύνης γνωστοποιούν στην ΕΕΤΤ, σύμφωνα με τα οριζόμενα στο Άρθρο 7 του παρόντος, τον τερματισμό των εργασιών τους. Ο τερματισμός εργασιών σημειώνεται στο ηλεκτρονικό αρχείο της ΕΕΤΤ.

3.7. Οι Πάροχοι Υπηρεσιών Εμπιστοσύνης υποχρεούνται στην καταβολή ετήσιου τέλους ύψους εκατό ευρώ (€100). Το ως άνω τέλος για κάθε ημερολογιακό έτος θα καταβάλλεται εντός του τελευταίου τριμήνου του αμέσως προηγουμένου έτους.

Με σχόλια [DZ8]: Τι θα συμβεί αν δεν πληρωθεί το ετήσιο τέλος;

Άρθρο 4

Απαιτήσεις ασφάλειας για τους παρόχους υπηρεσιών εμπιστοσύνης

Με σχόλια [DZ9]: Να προστεθεί μια εισαγωγική παράγραφος που να αναφέρει «Σε συνέχεια των διατάξεων που αναφέρονται στο Άρθρο 19 του Κανονισμού…»

4.1. Οι πάροχοι υπηρεσιών εμπιστοσύνης, εγκεκριμένοι και μη, λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα διαχείρισης των κινδύνων για την ασφάλεια των υπηρεσιών εμπιστοσύνης που παρέχουν. Τα ανωτέρω θα πρέπει να περιγράφονται στην Αναφορά εκτίμησης κινδύνων και μέτρων αντιμετώπισης των περιστατικών ασφάλειας (Παράρτημα 3) και να είναι διαθέσιμα ανά πάσα στιγμή.

4.2. Οι πάροχοι υπηρεσιών εμπιστοσύνης, 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. Σημαντικός αντίκτυπος θεωρείται ότι υπάρχει όταν λάβει χώρα συμβάν με επίπεδο επίδρασης 3 ή μεγαλύτερο, σύμφωνα με τα οριζόμενα στο επόμενο Άρθρο 5. Η υποχρέωση αναφοράς αφορά σε όλες τις υπηρεσίες εμπιστοσύνης εγκεκριμένες και μη.

Με σχόλια [DZ10]: Στη διεθνή βιβλιογραφία, η ασφάλεια ορίζεται ως επίπτωση στην Ιδιωτικότητα (Confidentiality), Ακεραιότητα (Integrity), Διαθεσιμότητα (Availability). Ο,τιδήποτε επηρεάζει αυτές τις τρεις συνιστώσες, επηρεάζει την «ασφάλεια». Κατά συνέπεια, είναι πλεονασμός το να αναφερθεί στην ίδια πρόταση «η ασφάλεια ή απώλεια της ακεραιότητας» διότι η «ακεραιότητα» περιλαμβάνεται στην «ασφάλεια». Προτείνεται η διατύπωση:
«οποιαδήποτε παραβίαση της ασφάλειας (ιδιωτικότητα, ακεραιότητα, διαθεσιμότητα) που έχει σημαντικό αντίκτυπο…»

4.3. Οι πάροχοι υπηρεσιών εμπιστοσύνης, 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.

4.4. Οι πάροχοι υπηρεσιών εμπιστοσύνης, εγκεκριμένοι και μη, ενημερώνουν το κοινό, χωρίς αδικαιολόγητη καθυστέρηση για συμβάντα με επίπεδο επίδρασης τρία (3) ή μεγαλύτερο.

4.5. Οι πάροχοι υπηρεσιών εμπιστοσύνης, εγκεκριμένοι και μη, οφείλουν να έχουν διαθέσιμη ανά πάσα στιγμή αναφορά εκτίμησης κινδύνων και μέτρων αντιμετώπισης των περιστατικών ασφάλειας.

Άρθρο 5

Υποχρέωση αναφοράς συμβάντων στην ΕΕΤΤ

5.1. 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

Με σχόλια [DZ11]: Η υπάρχουσα διατύπωση είναι προβληματική ή έστω ανεφάρμοστη για τις περιπτώσεις ολιγόλεπτων διακοπών στην παροχή κάποιων υπηρεσιών. Αν μια υπηρεσία διακοπεί για λίγα λεπτά, ναι μεν επηρεάζεται αλλά όχι σημαντικά. Προτείνεται η διατύπωση «επηρεάζεται μέρος των πελατών/υπηρεσιών σε σημαντικό βαθμό»

5.2. Οι πάροχοι υπηρεσιών εμπιστοσύνης οφείλουν να αναφέρουν στην ΕΕΤΤ μόνο τα συμβάντα με επίπεδο επίδρασης τρία (3) ή μεγαλύτερο. Ενδεικτικά συμβάντα επιπέδου τρία (3) και άνω, τα οποία θα πρέπει να αναφέρονται από τους παρόχους θεωρούνται τα εξής:

Με σχόλια [DZ12]: Προτείνεται να δοθεί έστω ενδεικτική αξιολόγηση από την ΕΕΤΤ για κάθε ένα από τα παρακάτω συμβάντα. Βλ. προηγούμενο σχόλιο για το Άρθρο 4, παράγραφος 4.2 σε σχέση με την διαθεσιμότητα.

5.2.1. Αποθήκευση ιδιωτικού κλειδιού: π.χ. μη εξουσιοδοτημένη πρόσβαση σε:

i. Τα ιδιωτικά κλειδιά της Root CA
ii. Τα ιδιωτικά κλειδιά Sub CA
iii. Ιδιωτικά κλειδιά για την υπογραφή ~~πιστοποιητικών,~~ CRL, απαντήσεις OCSP
iv. Ιδιωτικά ~~Κ~~κλειδιά για τη λειτουργία της εγκεκριμένης υπηρεσίας εμπιστοσύνης (πχ Χρονοσήμανσης)
v. ~~Μη εξουσιοδοτημένη πρόσβαση στα~~ ιδιωτικά κλειδιά των τελικών χρηστών λόγω των 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

5.2.2. Έκδοση πιστοποιητικών: Κλεμμένα πιστοποιητικά
5.2.3. Κλοπή ταυτότητας: Ο επιτιθέμενος κάνει ψευδή αξίωση ταυτότητας, αποκτά πιστοποιητικά για διαφορετική ταυτότητα.
5.2.4. Αναίρεση αίτησης εμπιστοσύνης: σφάλμα λογισμικού ή υλικού που προκαλεί διακοπή της υπηρεσίας απόκρισης ανάκλησης
5.2.4.1. Αποτυχία του παρόχου να δεχτεί ή να επεξεργαστεί τα αιτήματα ανάκλησης
5.2.4.2. Αποτυχία διάθεσης πληροφορίας για τη διαθεσιμότητα ή ανάκληση εγκεκριμένων πιστοποιητικών (μη διαθεσιμότητα της υπηρεσίας CRL/OCSP)
5.2.5. Παραβιάσεις ασφαλείας που οδηγούν σε παραβίαση προσωπικών δεδομένων, πελατών ή άλλων μερών, όπως οι υπάλληλοι ή οι σύμβουλοι του παρόχου
5.2.6. Μη διαθεσιμότητα της υποδομής αποθήκευσης δημόσιου κλειδιού (πιστοποιητικά Root και Sub CA)
5.2.7. Μη διαθέσιμη υπηρεσία χρονοσφραγίδας
5.2.8. Έκδοση εγκεκριμένων πιστοποιητικών χωρίς τη χρήση αξιόπιστων συστημάτων σύμφωνα με το άρθρο 24 (2) και (5) του Κανονισμού eIDAS
5.2.9. Υποβαθμισμένη ή μη διαθέσιμη υπηρεσία εμπιστοσύνης, π.χ. όπου χρησιμοποιούνται διακομιστές υπογραφής ή δίκτυο/κεντρικό σύστημα αποθήκευσης κλειδιού
5.2.10. Μη εξουσιοδοτημένη πρόσβαση σε, διαγραφή ή αλλαγή των προσωπικών δεδομένων των πελατών του παρόχου
5.2.11. Περιστατικά ασφαλείας που οδηγούν σε παραβίαση της ασφάλειας των επικοινωνιών, οδηγώντας σε παραβιάσεις της ιδιωτικής ζωής

5.3. 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) και στη συνέχεια, σε μεταγενέστερο στάδιο, όταν εντοπίζονται τα στοιχεία του συμβάντος, παρέχει μια πιο λεπτομερή και περιγραφική κοινοποίηση (τελική δήλωση συμβάντος).

5.4. Οι πληροφορίες που πρέπει τουλάχιστον να περιλαμβάνονται σε μια ειδοποίηση συμβάντος είναι:

Αρχική δήλωση συμβάντος

1. Ημερομηνία και ώρα κατά την οποία το περιστατικό ασφαλείας εντοπίστηκε (ή ξεκίνησε εάν είναι γνωστό)
2. Στοιχεία επικοινωνίας: Στοιχεία επικοινωνίας για ερωτήσεις σχετικά με αυτό το περιστατικό ασφάλειας
3. Σχετικός πάροχος: επωνυμία της εταιρείας

Με σχόλια [DZ13]: Επίπεδο 5?

Με σχόλια [DZ14]: Επίπεδο 4?

Με σχόλια [DZ15]: Επίπεδο 4?

Με σχόλια [DZ16]: Επίπεδο 3 ή 4?

Με σχόλια [DZ17]: Επίπεδο 3 ή 4?

Με σχόλια [DZ18]: Είναι ασαφές. Το ιδιωτικό κλειδί είναι πάντα υπό τον έλεγχο του κατόχου/συνδρομητή. Αν ένας Τρίτος ζητήσει και καταφέρει την έκδοση νέου Πιστοποιητικού χωρίς να έχει πρόσβαση στο ιδιωτικό κλειδί που σχετίζεται με το Πιστοποιητικό, δεν μπορεί να χαρακτηρίζεται πρόβλημα ασφάλειας κατηγορίας 3 και πάνω. Γενικά το παράδειγμα δεν είναι πολύ σαφές. Προτείνεται αναδιατύπωση ή αφαίρεση.

Με σχόλια [DZ19]: Η πρόταση διαβάζεται ως «μη εξουσιοδοτημένη πρόσβαση σε Μη ανακτήσιμη καταστροφή ιδιωτικών κλειδιών». Προτείνεται να έχει ξεχωριστή αρίθμηση και περιγραφή «καταστροφή ιδιωτικών κλειδιών από ενεργές (μη ληγμένες και μη ανακλημένες) Αρχές Πιστοποίησης, χωρίς δυνατότητα ανάκτησης των κλειδιών», το οποίο φαίνεται να είναι πρόβλημα επιπέδου 4 ή 5 αν αφορά ιδιωτικό κλειδί κάποιας RootCA.

Με σχόλια [DZ20]: Δεν είναι σαφές ποιο είναι το συμβάν. Τα Ψηφιακά Πιστοποιητικά είναι κατά κανόνα δημόσια. Προτείνουμε την αφαίρεση του παραδείγματος.

Με σχόλια [DZ21]: Επίπεδο 3?

Με σχόλια [DZ22]: Επίπεδο 3?

Με σχόλια [DZ23]: Δεν είναι εύκολη η κατάταξη ως έχει. Σύμφωνα με τις τυπικές συμβάσεις συνδρομητών και κειμένων πολιτικής/διαδικασιών των Παρόχων, τα Relying Parties δεν πρέπει να εμπιστεύονται τα Πιστοποιητικά συνδρομητών αν δεν ελέγξουν τα CRLs ή τα OCSP responses. Αν υπάρχει ταυτόχρονη διακοπή στην υπηρεσία CRL και OCSP, το Relying Party θα δοκιμάσει αργότερα. Στιγμιαία ή ολιγόλεπτη **ταυτόχρονη** διακοπή παροχής των υπηρεσίας CRL KAI OCSP δεν θα πρέπει να χαρακτηρίζεται αυτόματα ως περιστατικό ασφάλειας. Προτείνεται να προστεθεί στο παράδειγμα ένα ενδεικτικό διάστημα διακοπής πχ «Αποτυχία διάθεσης πληροφορίας για την κατάσταση εγκυρότητας εγκεκριμένων πιστοποιητικών για περισσότερο από 3+ ώρες (ταυτόχρονη μη διαθεσιμότητα των υπηρεσιών CRL KAI OCSP)».

Με σχόλια [DZ24]: Αν πρόκειται για συνδρομητές, φαίνεται να είναι πρόβλημα επιπέδου 3. Αν πρόκειται για προσωπικό του Παρόχου, φαίνεται να είναι πρόβλημα επιπέδου 2. Συνεπώς, προτείνουμε να γίνει «Παραβιάσεις ασφαλείας που οδηγούν σε παραβίαση προσωπικών δεδομένων συνδρομητών».

Με σχόλια [DZ25]: Τα Πιστοποιητικά Root και SubCAs είναι κατά κανόνα δημόσια. Οι συνδρομητές που χρησιμοποιούν τα τελικά τους πιστοποιητικά για πράξεις υπογραφής, οφείλουν να παραδίδουν την αλυσίδα Πιστοποιητικών στους παραλήπτες. Η μη διαθεσιμότητα των δημόσιων κλειδιών Root και SubCA δεν προκαλεί κάποιο πρόβλημα ώστε να χαρακτηριστεί περιστατικό, πόσο μάλλον περιστατικό ασφάλειας κατηγορίας 3 και πάνω. Προτείνεται να αφαιρεθεί το παράδειγμα.

Με σχόλια [DZ26]: Το συγκεκριμένο φαίνεται να είναι πρόβλημα επιπέδου 2. Δεν επηρεάζει τον συνδρομητή ο οπο... [1]

Με σχόλια [DZ27]: Πρόβλημα επιπέδου 3?

Με σχόλια [DZ28]: Φαίνεται να είναι πρόβλημα επιπέδου 2 λόγω του ότι ο χρήστης θα είναι δυσαρεστημένος με τη μη διαθεσιμότητα. Δεν επηρεάζει άμεσα τον συνδρομητή ο οπο... [2]

Με σχόλια [DZ29]: Φαίνεται να είναι πρόβλημα επιπέδου 2 και σε κάθε περίπτωση υπάρχει δυνατότητα ανάκτησης από αντίγραφα ασφαλείας. Δεν επηρεάζεται ο συνδρομητής ο οποίος έχει ήδ... [3]

4. Υπηρεσίες εμπιστοσύνης που επηρεάζονται (ή πιθανώς επηρεάζονται): περιγραφή της/των υπηρεσίας (ών)
5. Τα προσωπικά δεδομένα που επηρεάστηκαν (ή ενδεχομένως επηρεάστηκαν) και περιγραφή αυτών
6. Σύντομη περιγραφή του συμβάντος ασφαλείας
7. Μέτρα που ελήφθησαν ή προγραμματίστηκαν
8. Διασυνοριακές επιπτώσεις

Τελική δήλωση συμβάντος

1. Ημερομηνία και ώρα έναρξης του περιστατικού ασφαλείας
2. Ημερομηνία και ώρα που το περιστατικό ασφαλείας εντοπίστηκε από τον πάροχο
3. Διάρκεια του συμβάντος σε ώρες: η χρονική περίοδος μεταξύ της στιγμής κατά την οποία η υπηρεσία αρχίζει να υποβαθμίζεται και της στιγμής όταν η υπηρεσία είναι πάλι διαθέσιμη στον τελικό χρήστη ή το χρονικό διάστημα κατά το οποίο ο τελικός χρήστης δεν μπόρεσε να χρησιμοποιήσει την υπηρεσία
4. Στοιχεία επικοινωνίας: Στοιχεία επικοινωνίας για ερωτήσεις σχετικά με αυτό το περιστατικό ασφάλειας
5. Σχετικός πάροχος: επωνυμία της εταιρείας
6. Σοβαρότητα του συμβάντος: Η σοβαρότητα των συμβάντων ασφαλείας βαθμολογείται σε κλίμακα από 1 έως 5. Μόνο τα περιστατικά επιπέδου σοβαρότητας 3 και πάνω είναι ανακοινώσιμα.
   6.1. Επίπεδο 1. Χωρίς επιπτώσεις
   6.2. Επίπεδο 2. Ασήμαντες επιπτώσεις: Επηρεάστηκαν τα περιουσιακά στοιχεία του παρόχου αλλά δεν επηρεάστηκαν οι βασικές υπηρεσίες
   6.3. Επίπεδο 3. Σημαντικός αντίκτυπος: επηρεάζεται μέρος των πελατών / υπηρεσιών
   6.4. Επίπεδο 4. Σοβαρός αντίκτυπος: επηρεάζεται μεγάλο μέρος των πελατών / υπηρεσιών
   6.5. Επίπεδο 5. Καταστροφικές επιπτώσεις: ολόκληρη η οργάνωση, όλες οι υπηρεσίες, όλα τα πιστοποιητικά επηρεάζονται
7. Αριθμός και ποσοστό πελατών που επηρεάστηκαν
8. Γενική περιγραφή του συμβάντος ασφαλείας: Για παράδειγμα, επηρεάζονται συστήματα πληροφορικής, πώς εντοπίστηκε το συμβάν, πόσο καιρό το περιστατικό ήταν ενεργό, υπάρχει ευπάθεια στο λογισμικό που περιλαμβάνει τρίτο μέρος κλπ
9. Υπηρεσίες εμπιστοσύνης που επηρεάζονται (ή πιθανώς επηρεάζονται): περιγραφή της/των υπηρεσίας (ών) (Παραρτήματα 1 και 2).
10. Κατηγορία υπηρεσίας εμπιστοσύνης που επηρεάστηκε: εγκεκριμένη ή μη εγκεκριμένη
11. Χαρακτηριστικά ασφαλείας που επηρεάζονται: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα
12. Τα δεδομένα προσωπικού χαρακτήρα που επηρεάστηκαν και περιγραφή αυτών
13. Λεπτομερή στοιχεία που επηρεάστηκαν: πλατφόρμα Αρχής Πιστοποίησης (CA), πλατφόρμα Αρχής Εξουσιοδότησης (VA), πλατφόρμα Αρχής Χρονοσφραγίδας (TSA), Πλατφόρμα Αρχής Εγγραφής (RA), πλατφόρμα δημιουργίας και επικύρωσης υπογραφών / σφραγίδων, πλατφόρμα διατήρησης υπογραφών / σφραγίδων, πλατφόρμα υπηρεσίας συστημένης παράδοσης, πλατφόρμα δικτύου, αρχείο, υλικό, λογισμικό, άλλα
14. Βαθμός επιρροής στοιχείων: χαμηλός, μέσος, υψηλός (όπως έχει δημοσιευθεί στο: https://www.enisa.europa.eu/publications/article19-incident-reporting-framework)
15. Κατηγορία αιτίας:
    15.1. ανθρώπινο λάθος,
    15.2. κακόβουλες ενέργειες,

Με σχόλια [DZ30]: Δεν υπάρχουν ορισμοί για τα CA, VA, TSA, RA κλπ. Ποια είναι η διαφορά VA και RA? Κάθε Πάροχος έχει ενδεχομένως διαφορετικούς ορισμούς για τα επιμέρους τμήματα που συνθέτουν τις υπηρεσίες εμπιστοσύνης. Προτείνεται να αντικατασταθεί με «Επιμέρους υποσυστήματα που επηρεάστηκαν. Ενδεικτικά αναφέρονται τα υποσυστήματα Αρχών Πιστοποίησης (CA), Αρχών Καταχώρησης (RA), Υπηρεσίες Χρονοσήμανσης (TSA), Υπηρεσίες ελέγχου κατάστασης πιστοποιητικών (CRL/OCSP), κ.α.» Στο Άρθρο 2 του παρόντος κανονισμού, προτείνεται να προστεθούν ορισμοί για τα CA, RA, TSA, CRL/OCSP.

15.3. φυσικές καταστροφές,
15.4. αποτυχία συστήματος,
15.5. αποτυχία τρίτων μερών.

16. Λεπτομερής περιγραφή της αιτίας παραβίασης ασφάλειας:
16.1. Επίθεση άρνησης εξυπηρέτησης (Denial of Service),
16.2. Κακόβουλο λογισμικό (Malware) και ιοί,
16.3. Κλοπή ή απώλεια εξοπλισμού,
16.4. Κλοπή ή απώλεια δεδομένων,
16.5. Διακοπή ρεύματος,
16.6. Αποτυχία υλικού,
16.7. Σφάλμα λογισμικού,
16.8. Ελαττωματική αλλαγή / ενημέρωση υλικού,
16.9. Ελαττωματική αλλαγή / ενημέρωση λογισμικού,
16.10. Παραβίαση προσωπικών δεδομένων,
16.11. Υποκλοπή,
16.12. Κρυπτοαναλύσεις,
16.13. Υπερφόρτωση,
16.14. Εσφαλμένη πολιτική ή διαδικασία,
16.15. Ασφάλεια τερματισμού λειτουργίας,
16.16. Άλλα
17. Εκτίμηση κόστους
18. Μέτρα που ελήφθησαν για τον μετριασμό του συμβάντος
19. Μακροπρόθεσμα μέτρα, που έχουν ληφθεί ή προγραμματίζονται, ώστε να αποφευχθούν παρόμοια περιστατικά στο μέλλον
20. Διασυνοριακές επιπτώσεις
21. Άλλες Αρχές που ενημερώθηκαν
22. Ειδοποίηση ενδιαφερόμενων πελατών (ΝΑΙ/ΟΧΙ)
23. Δημόσια ενημέρωση (ΝΑΙ/ΟΧΙ)

Με σχόλια [DZ31]: Ασαφές γιατί υπάρχει κόστος αποζημιώσεων, κόστος αντικατάστασης, κόστος μη λειτουργίας της υπηρεσίας (απώλεια εσόδων), κ.α. Επιπλέον, η ζημία στη «φήμη» ενός οργανισμού δεν μπορεί να αξιολογηθεί. Θα μπορούσε να γίνει «Εκτίμηση ζημίας που έχουν υποστεί ο Πάροχος, οι συνδρομητές και τα έμπιστα τρίτα μέρη (Relying Parties)»

ΜΕΡΟΣ Γ': Υποχρεώσεις εγκεκριμένων Παρόχων Υπηρεσιών Εμπιστοσύνης (ΠΥΕ)

Άρθρο 6
Έναρξη εγκεκριμένων υπηρεσιών εμπιστοσύνης

6.1. Έγκριση στους ενδιαφερόμενους Παρόχους Υπηρεσιών Εμπιστοσύνης (ΠΥΕ) και στις υπηρεσίες που ενδιαφέρονται αυτοί να παρέχουν, χορηγείται από την ΕΕΤΤ, κατόπιν σχετικού αιτήματος των ενδιαφερομένων. Μη εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης που 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 πάροχοι υπηρεσιών εμπιστοσύνης που επιθυμούν την έναρξη νέας εγκεκριμένης υπηρεσίας εμπιστοσύνης.

6.2. Με την υποβολή του αιτήματος εκκινεί η Διαδικασία Έναρξης Παροχής Υπηρεσιών (διαδικασία «έναρξης εγκεκριμένη υπηρεσίας εμπιστοσύνης»), κατά την οποία η ΕΕΤΤ εξετάζει εάν ο πάροχος υπηρεσιών εμπιστοσύνης και οι παρεχόμενες από αυτόν υπηρεσίες εμπιστοσύνης συμμορφώνονται με τις απαιτήσεις του Κανονισμού eIDAS. Στην εν λόγω διαδικασία υποβάλλεται χωριστά κάθε υπηρεσία εμπιστοσύνης (από τις προβλεπόμενες στον Κανονισμό eIDAS) που επιθυμεί να παρέχει ο πάροχος υπηρεσιών εμπιστοσύνης και δεν έχει ακόμα εγκριθεί.

Ο υποψήφιος ΠΥΕ που αιτείται την έγκριση για παροχή εγκεκριμένων υπηρεσιών εμπιστοσύνης πρέπει να αποδεικνύει τη συμμόρφωσή του με τις απαιτήσεις του Κανονισμού eIDAS και της παρούσας Απόφασης και με κάθε άλλη ρύθμιση που αφορά στην έκδοση Εγκεκριμένων Πιστοποιητικών.

6.3. Ο υποψήφιος ΠΥΕ υποβάλει αίτηση εγγραφής στο ηλεκτρονικό αρχείο της ΕΕΤΤ, σύμφωνα με τα οριζόμενα στο Άρθρο 3 και επιπλέον συνυποβάλλει ηλεκτρονικά στην ΕΕΤΤ (Παράρτημα 4 της παρούσας Απόφασης) τα παρακάτω έγγραφα:

1. Έκθεση Αξιολόγησης της Συμμόρφωσης (ΕΑΣ) εκδοθείσα από Οργανισμό Αξιολόγησης της Συμμόρφωσης (Conformity Assessment Body -CAB) σύμφωνα με το Άρθρο 10 της παρούσας Απόφασης
2. Πιστοποιητικό εγγραφής στο Γενικό Εμπορικό Μητρώο (Γ.Ε.ΜΗ.)
3. Πιστοποιητικό 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 εταιρία κατά την ημερομηνία υποβολής της αίτησης (νόμιμος εκπρόσωπος, δικαίωμα υπογραφής κλπ.), τυχόν τρίτοι, στους οποίους έχει χορηγηθεί εξουσία εκπροσώπησης, καθώς και η θητεία του/των ή/και των μελών του οργάνου διοίκησης/ νόμιμου εκπροσώπου.
4. 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.
5. Δείγματα (Test samples) των πιστοποιητικών ή άλλων στοιχείων που θα εκδοθούν ή θα δημιουργηθούν ως μέρος της υπό έγκριση υπηρεσίας.
6. Έγγραφο σχετικά με την αποτίμηση κινδύνου σύμφωνα με τις απαιτήσεις του Άρθρου 19.1 του Κανονισμού eIDAS (eIDAS Regulation Art.19.1) (Παράρτημα 3 της παρούσας Απόφασης).
7. Σχέδιο Ειδοποίησης του τελικού χρήστη, σε περίπτωση αθέτησης της επαρκούς προστασίας της ασφάλειας και των προσωπικών δεδομένων, σύμφωνα με τις απαιτήσεις του Άρθρου 19.2 του Κανονισμού eIDAS (eIDAS Regulation Art.19.2).
8. Σχέδιο Τερματισμού λειτουργίας του εν λόγω Παρόχου (Άρθρο 7 της παρούσας Απόφασης), σύμφωνα με τα Άρθρα 17.4.(~~ί~~θ) και 24.2.(i) του Κανονισμού eIDAS (eIDAS Regulation Art. 17.4.(i) και 24.2.(i)).
9. Αντίγραφο της τυποποιημένης Σύμβασης με τους τελικούς χρήστες (end users)

6.4. Η αίτηση και τα συνυποβαλλόμενα έγγραφα υποβάλλονται στην ΕΕΤΤ ηλεκτρονικά μέσω του συστήματος Ηλεκτρονικής Υποβολής Αιτήσεων για παρόχους. Τα έγγραφα υπ' αριθμ. 4, 6, 7, 8, 9 της παρούσας παραγράφου φέρουν την εγκεκριμένη ηλεκτρονική υπογραφή του ~~νομίμου~~νόμιμου εκπροσώπου του Παρόχου ή την εγκεκριμένη ηλεκτρονική σφραγίδα της αιτούσας εταιρείας. Για την πρόσβαση στο Σύστημα Ηλεκτρονικής Υποβολής Αιτήσεων ο αιτών υποβάλλει «Δήλωση Διαχειριστή» σύμφωνα με την Απόφαση ΕΕΤΤ ΑΠ 586/006/30-11-2010 «Καθορισμός Δήλωσης Διαχειριστή για χρήση Διαδικτυακής Εφαρμογής της ΕΕΤΤ» (ΦΕΚ 2052/Β/31-12-2010) όπως εκάστοτε ισχύει.

6.5. Η ηλεκτρονική υπογραφή ή σφραγίδα της αίτησης του υποψηφίου ΠΥΕ πρέπει να είναι συμβατή με την πρότυπη μορφή όπως αναφέρεται στην Εκτελεστική Απόφαση (ΕΕ) 2015/1506 (Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be ~~recognised~~recognized by public sector bodies pursuant to Articles 27(5) and 37(5)

Με σχόλια [DZ32]: Το έγγραφο αποτίμησης κινδύνου που αναφέρεται στο Άρθρο 19.1 του Κανονισμού, είναι εσωτερικό έγγραφο του Παρόχου το οποίο ελέγχεται από τον ΟΑΣ, ο οποίος δεσμεύεται από σύμβαση εχεμύθειας. Το έγγραφο αυτό περιέχει ευαίσθητες και εμπιστευτικές πληροφορίες και δεν πρέπει να κυκλοφορεί χωρίς τον απόλυτο έλεγχο του Παρόχου. Στον Κανονισμό, και ειδικά στο άρθρο 19.1 δεν υπάρχει υποχρέωση κοινοποίησης του συγκεκριμένου εγγράφου στην Εποπτεύουσα Αρχή ή σε κάποιον Τρίτο. Εμμέσως οφείλει ο Πάροχος να το παρουσιάσει στον Φορέα Πιστοποίησης διότι ο Φορέας Πιστοποίησης πρέπει να εκτιμήσει τη συμμόρφωση του Παρόχου στο Άρθρο 19.1 του Κανονισμού. Προτείνεται να αφαιρεθεί η υποχρέωση υποβολής του συγκεκριμένου εγγράφου στην ΕΕΤΤ.

Με σχόλια [DZ33]: Παρομοίως με το προηγούμενο σχόλιο. Σχέδιο πρέπει να υπάρχει, αξιολογείται από τον Φορέα Πιστοποίησης αλλά δεν προκύπτει υποχρέωση κοινοποίησης στην Εποπτεύουσα Αρχή ή σε άλλο Τρίτο φορέα.

Με σχόλια [DZ34]: Η συγκεκριμένη απαίτηση, προκύπτει σωστά από το Άρθρο 17.4 (θ) του Κανονισμού. Συνήθως, υπάρχει δημοσιευμένη μια περίληψη του σχεδίου που βρίσκεται στα κείμενα Πολιτικής Πιστοποίησης και Δήλωσης Διαδικασιών Πιστοποίησης. Αν ζητείται κάτι πιο αναλυτικό, όπως το σχέδιο που δίνεται στο Παράρτημα 5, τότε θα πρέπει τα κείμενα να χαρακτηριστούν ως «Εμπιστευτικά» καθώς θα περιλαμβάνουν κρίσιμες πληροφορίες για την ασφάλεια υποδομών και υπηρεσιών του Παρόχου. Η ΕΕΤΤ θα πρέπει να γνωστοποιήσει στους Παρόχους τα μέτρα που λαμβάνει (πολιτικές και πρακτικές) για τη διασφάλιση της εμπιστευτικότητας αυτών των πληροφοριών.

Με σχόλια [DZ35]: Όπως προαναφέραμε, εκτιμούμε ότι δεν προκύπτει υποχρέωση υποβολής ή κοινοποίησης των συγκεκριμένων εγγράφων/διαδικασιών προς την Εποπτεύουσα Αρχή ή Τρίτους φορείς, πέρα του Οργανισμού Αξιολόγησης της Συμμόρφωσης.

of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 235, 9.9.2015, p. 37–41.).

6.6. 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 ~~ποιό~~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 του σχετικού εγγράφου της ΕΕΤΤ. Η χρονική προθεσμία θα ορίζεται από την ΕΕΤΤ κατά περίπτωση και δεν θα 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.

6.7. Η ΕΕΤΤ δύναται να ζητήσει κατά περίπτωση επιπλέον στοιχεία και κάθε αναγκαία διευκρίνιση για τον έλεγχο της συμμόρφωσης του αιτούντος με τις απαιτήσεις του Κανονισμού eIDAS.

6.8. Η ΕΕΤΤ εξετάζει την ΕΑΣ και τα συνοδευτικά της έγγραφα, διαπιστώνει τη συμμόρφωση με τις σχετικές απαιτήσεις και αποφασίζει με αιτιολογημένη απόφασή της την χορήγηση, ή μη, έγκρισης του αιτούντα και των αιτούμενων υπηρεσιών, εντός προθεσμίας τριών (3) μηνών από την κοινοποίηση.

6.9. Εάν η εξέταση της συμμόρφωσης του υποψηφίου Παρόχου δεν ολοκληρωθεί εντός τριών (3) μηνών από την κοινοποίηση, η ΕΕΤΤ ενημερώνει σχετικά τον αιτούντα, εξηγώντας τους λόγους της καθυστέρησης και ορίζοντας προθεσμία εντός της οποίας θα ολοκληρωθεί η εξέταση της συμμόρφωσης.

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

α) Μη πληρότητα του φακέλου της υποβληθείσας αίτησης ή/και τυχόν περαιτέρω διευκρινίσεων σύμφωνα με την παρούσα Απόφαση,

β) Μη επαρκούς τεκμηρίωσης της πλήρωσης ενός ή περισσοτέρων εκ των ανωτέρω σημείων (1-9) βάσει των προσκομισθέντων εγγράφων, ή

γ) Μη πλήρωσης των απαιτήσεων που επιβάλλονται με βάση τον Κανονισμό ~~eIDAs~~eIDAS

Ο αιτών μπορεί να αρχίσει να παρέχει τις εγκεκριμένες υπηρεσίες εμπιστοσύνης μόνον αφού η έγκριση του καταχωριστεί και δημοσιευθεί στον Κατάλογο Εμπιστοσύνης της ΕΕΤΤ (Άρθρο 22 Κανονισμού eIDAS).

Από τα παραπάνω συνοδευτικά έγγραφα και ιδιαίτερα τα υπ' αριθμ. 1,4,6,7,8,9 πρέπει να είναι διαθέσιμα και στα Αγγλικά ώστε να διευκολυνθεί η συνεργασία μεταξύ των Μελών της Ένωσης.

Με σχόλια [DZ36]: Επαναλαμβάνουμε ότι δεν προκύπτει υποχρέωση κοινοποίησης των συγκεκριμένων εγγράφων από τον Κανονισμό προς την Εποπτεύουσα Αρχή.

Με σχόλια [DZ37]: Η υποχρέωση («πρέπει να») διαθεσιμότητας όλων αυτών των εγγράφων στα Αγγλικά, είναι αρκετά «επίπονη» για τους Παρόχους, ιδιαίτερα όταν η Ελληνική είναι Επίσημα αναγνωρισμένη Γλώσσα της Ευρωπαϊκής Ένωσης. Επιπλέον, το αναλυτικό σχέδιο Τερματισμού Λειτουργίας του Παρόχου δεν είναι δημόσιο έγγραφο για να υπάρχει υποχρέωση μετάφρασης εκτός αν εννοείται η περίληψη του σχεδίου. Μια περίληψη του σχεδίου τερματισμού βρίσκεται συνήθως στο δημόσιο κείμενο Πολιτικής Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης. Προτείνουμε σε πρώτη φάση εφαρμογής του νέου Κανονισμού της ΕΕΤΤ να γίνει ως εξής:
«Το έγγραφο 1 πρέπει να είναι διαθέσιμο και στην Αγγλική Γλώσσα. Συνίσταται τα έγγραφα 4 και 9 να είναι διαθέσιμα και στην Αγγλική Γλώσσα ώστε να διευκολυνθεί η συνεργασία μεταξύ των Μελών της Ευρωπαϊκής Ένωσης».

Άρθρο 7
Υποβολή σχεδίου τερματισμού εργασιών

7.1. Κάθε εγκεκριμένος ΠΥΕ οφείλει να διατηρεί ενημερωμένο Σχέδιο Τερματισμού Εργασιών, σύμφωνα με το Άρθρο 24 παράγραφος 2 στοιχείο (θ) του Κανονισμού eIDAS, με σκοπό την εξασφάλιση της συνέχειας της υπηρεσίας.

7.2. Κάθε εγκεκριμένος ΠΥΕ υποβάλει το Σχέδιο Τερματισμού Εργασιών προς έγκριση στην ΕΕΤΤ κατά την έναρξη των εργασιών του. Το σχέδιο τερματισμού εργασιών αξιολογείται από τον Οργανισμό Αξιολόγησης Συμμόρφωσης (ΟΑΣ) και η αξιολόγησή του περιλαμβάνεται στην έκθεση αξιολόγησης συμμόρφωσης του ΠΥΕ.

Με σχόλια [DZ38]: Ισχύει μόνο για τους ΠΥΕ κατά την έναρξη των εργασιών; Αν δεν ισχύει για τους υφιστάμενους ΠΥΕ, ίσως πρέπει να αναφερθεί πιο ρητά, διαφορετικά αφήνει περιθώριο διαφορετικών ερμηνειών.

7.3. 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 διενεργεί ελέγχους προκειμένου να επαληθεύσει την ύπαρξη και την συμμόρφωση (ορθή εφαρμογή των διατάξεων) του σχεδίου τερματισμού.

Με σχόλια [DZ39]: Έρχεται σε αντίφαση με το 7.2 γιατί δεν προκύπτει η υποχρέωση των υφιστάμενων Παρόχων να υποβάλλουν το Σχέδιο Τερματισμού Εργασιών στην ΕΕΤΤ. Υποθέτουμε ότι όπου αναφέρεται «Σχέδιο Τερματισμού», εννοείται το «Σχέδιο Τερματισμού που καλύπτει τις απαιτήσεις του Άρθρου 7 του παρόντος Κανονισμού της ΕΕΤΤ». Αυτό δεν είναι ένα «δημόσιο» έγγραφο αλλά εσωτερικό και εμπιστευτικό εκτός αν αφορά μόνο την περίληψη του σχεδίου που δεν περιέχει εμπιστευτικές πληροφορίες.

7.4. 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 υπηρεσία καταχωρημένη στον κατάλογο Εμπιστοσύνης (π.χ. περίοδος χρήσης του ιδιωτικού κλειδιού κλπ).

(Β) [Προγραμματισμένη], αλλά αναμενόμενη παύση των υπηρεσιών (π.χ. για επιχειρηματικούς λόγους κ.λπ.) και δημιουργία ή παροχή στους συνδρομητές αλλά νέων Υπηρεσιών

i. από τον ίδιο ΠΥΕ
ii. από τρίτο πάροχο
iii. από την ΕΕΤΤ ή τρίτων

(Γ) [Προγραμματισμένη] Ανάληψη, 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.

7.5. Το σχέδιο τερματισμού θα πρέπει να καλύπτει, τουλάχιστον, την εκούσια και ακούσια διακοπή των δραστηριοτήτων, την παύση μιας, περισσότερων ή όλων των υπηρεσιών από πάροχο, την ενδεχόμενη ανάληψη των δραστηριοτήτων που διακόπηκαν από ένα τρίτο μέρος ή άλλως την επίδοσή τους στην ΕΕΤΤ και να διασφαλίζει τη διατήρηση και τη διαθεσιμότητα των πληροφοριών που αναφέρονται στο σημείο Άρθρο 24 παράγραφος 2 στοιχείο (η) του Κανονισμού eIDAS, σύμφωνα με τις διατάξεις του άρθρου αυτού.

7.6. Το σχέδιο τερματισμού θα πρέπει να προβλέπει τόσο τον εκούσιο όσο και τον ακούσιο τερματισμό και να:

1. καθορίζει τον αντίκτυπο του τερματισμού στις σχετικές καταχωρίσεις του Εθνικού Καταλόγου Εμπιστοσύνης.
2. προβλέπει διαδικασίες για τη διαθεσιμότητα και προσβασιμότητα των αρχείων του Παρόχου σύμφωνα με τις υποχρεώσεις του Άρθρου 12 περί Τήρησης Αρχείου.
3. προβλέπει την ενημέρωση των εμπλεκομένων μερών που ενδεχόμενα επηρεάζονται από τον τερματισμό.

7.7. Το σχέδιο τερματισμού θα πρέπει τουλάχιστον να περιγράφει:

1. Διαδικασίες τερματισμού.
2. Διαδικασίες και σενάρια δοκιμών τερματισμού.
3. Εκπαίδευση σε διαδικασίες τερματισμού (συμπεριλαμβανομένης της δοκιμής).
4. Εκθέσεις δοκιμών διαδικασιών τερματισμού.
5. Επίσημες αναφορές ελέγχου διαδικασιών τερματισμού.
6. Επίσημες συμφωνίες τερματισμού (συμβατικές) με τρίτους (συμπεριλαμβανομένων των υπεργολάβων κ.λπ.).
7. Τους όρους και τις συνθήκες της εν λόγω υπηρεσίας, τις πρακτικές και τα έγγραφα πολιτικής.

7.8. Στο Παράρτημα 5 παρατίθεται προτεινόμενος πίνακας περιεχομένων για το σχέδιο τερματισμού.

Με σχόλια [DZ40]: «Προτεινόμενος» σημαίνει όχι υποχρεωτικός. Προτείνουμε να γίνει υποχρεωτική απαίτηση ώστε να υπάρχει ομοιόμορφη αντιμετώπιση/αξιολόγηση των Παρόχων έναντι του Ελληνικού Κανονισμού.

Άρθρο 8
Υποχρέωση γνωστοποίησης τερματισμού εργασιών

Με σχόλια [DZ41]: Στις εργασίες περιλαμβάνονται όλες οι Υπηρεσίες Εμπιστοσύνης, όχι μόνο η υπηρεσία Ψηφιακών Πιστοποιητικών.

Σε περίπτωση τερματισμού, εκούσιου ή ακούσιου, των εργασιών του, ο εγκεκριμένος ΠΥΕ έχει τις ακόλουθες υποχρεώσεις :

Με σχόλια [DZ42]: Όλο το άρθρο αφορά μόνο τους «εγκεκριμένους» ΠΥΕ ή γενικά όλους τους ΠΥΕ; Δεν υπάρχει πλήρης εναρμόνιση στα κείμενα που ακολουθούν. Αλλού αναφέρεται ως «ΠΥΕ», αλλού ως «ΠΥΕ Εγκεκριμένων Πιστοποιητικών», αλλού ως «Εγκεκριμένος ΠΥΕ». Αν χρησιμοποιήσουμε τους ορισμούς του Κανονισμού 910/2014, θα πρέπει παντού να υπάρχει η φράση «εγκεκριμένος ΠΥΕ». Αν κάποιες διατάξεις αφορούν και τους «μη-εγκεκριμένους» παρόχους, αυτό πρέπει να φαίνεται ευκρινώς.

Με σχόλια [DZ43]: «Δικαιούχος» είναι το φυσικό πρόσωπο που «δικαιούται» να αποκτήσει πρόσβαση σε μια Υπηρεσία Εμπιστοσύνης (πχ δικαιούται να αποκτήσει ένα ψηφιακό πιστοποιητικό για ηλεκτρονική υπογραφή. Δεν σημαίνει ότι έχει λάβει το πιστοποιητικό ή ότι είναι συνδρομητής. Ο Δικαιούχος, αφού περάσει τη διαδικασία αίτησης, έγκρισης, αποδοχής της σύμβασης συνδρομητή, απόκτησης Πιστοποιητικού/Υπηρεσίας, **τότε μετατρέπεται σε «κάτοχο Πιστοποιητικού/Συνδρομητή»** που διαθέτει Πιστοποιητικό ή πρόσβαση σε Υπηρεσία Εμπιστοσύνης. Προτείνεται να αλλάξει η διατύπωση από «Δικαιούχο» σε «Συνδρομητή» και από «Δικαιούχο Πιστοποιητικού» σε «Κάτοχο/Συνδρομητή Υπηρεσίας Εμπιστοσύνης».

Με σχόλια [DZ44]: Δυσνόητο κείμενο.

α. γνωστοποιεί άμεσα τον τερματισμό προς την ΕΕΤΤ, τους ~~δικαιούχους~~ συνδρομητές Υπηρεσιών Εμπιστοσύνης ~~των Πιστοποιητικών~~ και κάθε Πάροχο Υπηρεσιών Εμπιστοσύνης ή άλλον με τον οποίο έχει συνάψει σύμβαση ή έχει οποιαδήποτε άλλη σχέση στα πλαίσια της ~~Π~~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 εργασιών του. Με την έκδοση και δημοσίευση της σχετικής απόφασης, ο ΠΥΕ υποχρεούται να ενημερώσει όσους αναφέρονται στο εδάφιο α΄ του παρόντος άρθρου,

γ. σε κάθε περίπτωση, ο ΠΥΕ φέρει το βάρος απόδειξης γνωστοποίησης του τερματισμού των εργασιών του στην ΕΕΤΤ, στους ~~δικαιούχους~~ συνδρομητές των ~~πιστοποιητικών~~ υπηρεσιών εμπιστοσύνης και σε κάθε ΠΥΕ ή άλλον με τον οποίο έχει συνάψει σύμβαση ή έχει οποιαδήποτε άλλη σχέση στα πλαίσια της παροχής υπηρεσιών εμπιστοσύνης,

δ. στην περίπτωση όπου δεν είναι δυνατόν για έναν εγκεκριμένο ΠΥΕ να μεταφέρει τις δραστηριότητες σε άλλο εγκεκριμένο Πάροχο για τη συνέχιση των εν λόγω υπηρεσιών με το δικό του όνομα, ο ΠΥΕ προβαίνει άμεσα στην ακύρωση όλων των σε ισχύ πιστοποιητικών. Αυτό θα απαιτήσει de facto την παύση παροχής οποιασδήποτε υπηρεσίας,

Με σχόλια [DZ45]: Δεν λαμβάνεται μέριμνα για τις υπηρεσίες ελέγχου εγκυρότητας πιστοποιητικών (CRLs, OCSP). Το να ανακληθούν όλα τα Πιστοποιητικά και να μην είναι διαθέσιμη η πληροφορία ανάκλησης, δημιουργεί σοβαρό πρόβλημα ασφάλειας στα Relying Parties. Κατά τη γνώμη μας, σε περίπτωση αδυναμίας παροχής υπηρεσίας ελέγχου κατάστασης Πιστοποιητικών από τον Εγκεκριμένο Πάροχο, η ΕΕΤΤ πρέπει να αναλάβει την υποχρέωση δημοσίευσης των CRLs του υπό τερματισμό Παρόχου, αποκτώντας έλεγχο στις διευθύνσεις που βρίσκονται στην επέκταση CRLDP (Certificate Revocation List Distribution Points) μέσα στα Πιστοποιητικά που έχουν εκδοθεί. Από τη στιγμή που όλα τα Πιστοποιητικά έχουν ανακληθεί, το CRL θα μπορεί να έχει ημερομηνία λήξης μακριά στο μέλλον ώστε να μην απαιτείται η έκδοση νέου.

ε. ο εγκεκριμένος ΠΥΕ ~~Εγκεκριμένων Πιστοποιητικών~~, σε κάθε περίπτωση, υποχρεούται να έχει ήδη συμφωνήσει εγγράφως με άλλον εγκεκριμένο ~~Πάροχο Υπηρεσιών Εμπιστοσύνης Εγκεκριμένων Πιστοποιητικών~~ΠΥΕ, για την παράδοση στον τελευταίο του ~~α~~Αρχείου (ηλεκτρονικό και φυσικό) που τηρεί σύμφωνα με το Άρθρο XXX 12 της παρούσας. Η μη τήρηση αυτής της υποχρέωσης δύναται να

Μορφοποιήθηκε: Επισήμανση

επιφέρει την επιβολή των κυρώσεων που προβλέπονται στην παρούσα. Ο εγκεκριμένος ΠΥΕ, δέκτης, ο οποίος σύμφωνα με τα ανωτέρω παραλαμβάνει και διατηρεί το ~~αρχείο~~ Αρχείο εγκεκριμένου ~~Παρόχου Υπηρεσιών Εμπιστοσύνης~~ ΠΥΕ (δότη) λόγω την παύσης εργασιών του τελευταίου, οφείλει εντός επτά (7) ημερών από την ανάληψη του ~~αρχείου~~ Αρχείου να κοινοποιεί εγγράφως στην ΕΕΤΤ το γεγονός αυτό. Σε περίπτωση μη εφαρμογής των ανωτέρω και χωρίς περιορισμό τους, ο εγκεκριμένος ΠΥΕ του οποίου οι εργασίες παύουν, παραδίδει τ~~α~~ο εν λόγω ~~έγγραφα~~ Αρχείο (ηλεκτρονικό και φυσικό) καθώς και άλλα σχετικά στοιχεία προς φύλαξη στην ΕΕΤΤ, ενημερώνοντας σχετικά τους ~~δικαιούχους~~ συνδρομητές ~~πιστοποιητικών~~Υπηρεσιών Εμπιστοσύνης. Η ΕΕΤΤ δύναται να αναθέσει τη φύλαξη ~~των~~ του ανωτέρω ~~αρχείων~~ Αρχείου σε άλλο εγκεκριμένο ΠΥΕ ~~Εγκεκριμένων Πιστοποιητικών~~,

στ. σε κάθε περίπτωση, οι τυχόν συμβάσεις ανάθεσης σε τρίτους εκτέλεσης μέρους της διαδικασίας παροχής υπηρεσιών εμπιστοσύνης, λήγουν αυτοδικαίως με την παύση εργασιών του εγκεκριμένου ΠΥΕ. Για το σκοπό αυτό, οι συμβάσεις οι οποίες υπογράφονται μεταξύ εγκεκριμένου ΠΥΕ και τρίτων, περιλαμβάνουν όρο ο οποίος προβλέπει, επί ποινή ακυρότητας όλης της σύμβασης, την αυτοδίκαιη λύση της σε περίπτωση παύσης εργασιών του εγκεκριμένου ~~Παρόχου Υπηρεσιών Εμπιστοσύνης~~ΠΥΕ. Οι συμβάσεις οι οποίες υπογράφονται μεταξύ εγκεκριμένου ΠΥΕ ~~Εγκεκριμένων Πιστοποιητικών~~ και τρίτων, περιλαμβάνουν όρο ο οποίος προβλέπει, επί ποινή ακυρότητας όλης της σύμβασης, την υποχρέωση του τρίτου παράδοσης κατά τη διαδικασία του εδαφίου ζ του παρόντος άρθρου, του Α~~α~~ρχείου (φυσικό και ηλεκτρονικό) και όλων των εγγράφων και στοιχείων, που τυχόν κατέχει, ~~από/για~~σχετικά με την παροχή των Υπηρεσιών Εμπιστοσύνης, όπως για παράδειγμα το Αρχείο που σχετίζεται με την ~~–~~έκδοση και διαχείριση ~~των~~ εγκεκριμένων πιστοποιητικών για ηλεκτρονικές υπογραφές/σφραγίδες,

ζ. ο εγκεκριμένος ΠΥΕ υποχρεούται να έχει ρυθμίσει την οικονομική κάλυψη κάθε απαιτούμενης διαδικασίας και εκπλήρωσης υποχρεώσεων που προκύπτουν από την παύση των εργασιών του καθώς και ενδεχόμενης ζημίας που τυχόν προκληθεί σε ~~δικαιούχους~~ συνδρομητές Υπηρεσιών Εμπιστοσύνης~~πιστοποιητικών~~ ή 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. Η ΕΕΤΤ με Απόφασή της δύναται να ρυθμίσει ελάχιστο ποσό για την οικονομική και ασφαλιστική κάλυψη των ανωτέρω από τους εγκεκριμένους ΠΥΕ ~~Εγκεκριμένων Πιστοποιητικών~~. Σύμφωνα και με τα παραπάνω, ο εγκεκριμένος ΠΥΕ οφείλει να ενημερώσει άμεσα την ΕΕΤΤ για την πρόθεση τερματισμού της παροχής υπηρεσιών εν μέρει ή εξ ολοκλήρου. Όταν η ΕΕΤΤ ειδοποιηθεί από το ~~π~~Π άροχο ή από οποιονδήποτε εξουσιοδοτημένο τρίτο (π.χ. σε περίπτωση μη αναμενόμενου τερματισμού ή πτώχευσης), περί του τερματισμού ή της πρόθεσης να παύσει η παροχή των υπηρεσιών εν μέρει ή εξ ολοκλήρου, επαληθεύει την ύπαρξη, την συνεχή ενημέρωση/επικαιροποίηση και την ορθή εφαρμογή του σχεδίου τερματισμού, συμπεριλαμβανομένου του τρόπου με τον οποίο οι πληροφορίες

Με σχόλια [DZ46]: Ιδιαίτερα «περιοριστικό» νομικό κείμενο που υποδεικνύει στους Παρόχους πώς θα συνάπτουν συμβάσεις με Τρίτους. Προτείνεται να αντικατασταθεί με τα σημεία/προδιαγραφές που πρέπει να εξασφαλίζονται από τέτοιες συμβάσεις και όχι η ακριβής διατύπωση της σύμβασης.

παραμένουν προσβάσιμες σύμφωνα με το άρθρο 24 παράγραφος 2 (η) του Κανονισμού eIDAS. Η ΕΕΤΤ έχει την ευθύνη να διασφαλίσει ότι ο εγκεκριμένος ΠΥΕ ή/και οι υπηρεσίες έχουν παύσει κανονικά και όταν κρίνει ότι δεν πληρούνται πλέον τις απαιτήσεις του Κανονισμού eIDAS, αφαιρεί την έγκριση και ενημερώνει κατάλληλα τον Εθνικό Κατάλογο Εμπιστοσύνης.

Για την ορθή εφαρμογή του τερματισμού, ο εγκεκριμένος ΠΥΕ οφείλει να μεριμνήσει για την κατάλληλη κοινοποίηση της πρόθεσής του, και την διαφύλαξη και την προσβασιμότητα του Αρχείου (όπως ορίζεται στο Άρθρο 12 του παρόντος). Ειδικά για την περίπτωση Εγκεκριμένων Πιστοποιητικών για ηλεκτρονικές υπογραφές/σφραγίδες, η διαφύλαξη και η προσβασιμότητα πρέπει να ισχύει ~~των πιστοποιητικών,~~ για επτά (7) έτη από την ~~έκδοσή~~ λήξη ισχύος τους, ακόμη και μετά την παύση των δραστηριοτήτων του. Επίσης όλες οι σχετικές πληροφορίες σχετικά με τα δεδομένα που εκδίδονται και λαμβάνονται από τον εγκεκριμένο ΠΥΕ, θα 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.
Ο κίνδυνος μη ορθής εκτέλεσης του σχεδίου τερματισμού θα πρέπει να αποτελεί μέρος των κινδύνων που αναλύονται, αξιολογούνται σε σχέση με δραστηριότητες και διαδικασίες τερματισμού.

Άρθρο 9
Υποχρέωση υποβολής έκθεσης αξιολόγησης συμμόρφωσης

9.1. Ως Οργανισμούς Αξιολόγησης Συμμόρφωσης (ΟΑΣ) η ΕΕΤΤ αποδέχεται μόνο εκείνους τους φορείς που έχουν διαπιστευθεί, όπως απαιτείται από 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, που χορηγείται από τον Εθνικό Φορέα Διαπίστευσης του κράτους στο οποίο είναι εγκατεστημένος. Επιπλέον, η διαπίστευση πρέπει να υποδεικνύει ότι ο ΟΑΣ:

1. έχει την ικανότητα και τις επαρκείς γνώσεις για την αξιολόγηση του παρόχου με τις απαιτήσεις του κανονισμού eIDAS.
2. προαιρετικά, προσαρμόζεται στις απαιτήσεις του προτύπου ISO/IEC 17065: 2012.
3. προαιρετικά, προσαρμόζεται στις απαιτήσεις του προτύπου ETSI EN 319 403 v2.2.2 (2015-08).

Ειδικά για την Πιστοποίηση των Υπηρεσιών Εμπιστοσύνης:

- δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών υπογραφών (e-Signatures)
- δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών σφραγίδων (e-Seals)
- δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών χρονοσφραγίδων (Time Stamping)

~~3.~~ του κανονισμού eIDAS, η διαπίστευση πρέπει να υποδεικνύει ότι ο ΟΑΣ υποχρεωτικά προσαρμόζεται στις απαιτήσεις του προτύπου ETSI EN 319 403 v2.2.2 (2015-08) ή νεότερο.

9.2. Οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης ελέγχονται, με δικές τους δαπάνες τουλάχιστον κάθε 24 μήνες, από ΟΑΣ. Σκοπός του ελέγχου είναι να επιβεβαιώνεται ότι οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης και οι παρεχόμενες από αυτούς εγκεκριμένες υπηρεσίες εμπιστοσύνης πληρούν τις απαιτήσεις του παρόντος κανονισμού.

Με σχόλια [DZ47]: Τα 7 έτη σύμφωνα με το 12.6 ξεκινούν από τη λήξη των εγκεκριμένων πιστοποιητικών όχι από την έκδοσή τους.

Με σχόλια [DZ48]: Είναι κατανοητή η διάταξη για την προαιρετική διαπίστευση στα συγκεκριμένα πρότυπα, όσον αφορά τις υπηρεσίες e-Delivery και e-Preservation για τις οποίες δεν υπάρχουν εγκεκριμένα τεχνικά πρότυπα. Ειδικά όμως για την παροχή των Υπηρεσιών e-Signature, e-Seal, Time Stamping που υπάρχουν εγκεκριμένα τεχνικά πρότυπα, θεωρούμε προϋπόθεση για την σωστή εφαρμογή του Κανονισμού, να οριστεί υποχρεωτική η Διαπίστευση του ΟΑΣ στο πρότυπο ETSI EN 319 403. Στο ίδιο άρθρο (9.1), προτείνεται να προστεθεί κείμενο που να το υποστηρίζει.

Μορφοποιήθηκε: Ελληνικά

Μορφοποιήθηκε: Εσοχή: Αριστερά: 0,75 εκ., Χωρίς κουκκίδες ή αρίθμηση

Μορφοποιήθηκε: Κουκκίδα + Επίπεδο: 1 + Στοίχιση: 1,27 εκ. + Εσοχή: 1,9 εκ.

Μορφοποιήθηκε: Εσοχή: Αριστερά: 0,63 εκ., Χωρίς κουκκίδες ή αρίθμηση

Μορφοποιήθηκε: Ελληνικά

Μορφοποιήθηκε: Ελληνικά

Μορφοποιήθηκε: Ελληνικά

Μορφοποιήθηκε: Ελληνικά

Με σχόλια [DZ49]: Στο σημείο αυτό θα άξιζε να γίνει αναφορά στις Εγκεκριμένες Απομακρυσμένες Διατάξεις Δημιουργίας Υπογραφής (ΕΑΔΔΥ), στις περιπτώσεις που αυτές λειτουργούν στις εγκαταστάσεις Τρίτου Φορέα (μη Παρόχου).
Υποχρεωτικά, ο φορέας αυτός πρέπει να συμμορφώνεται (και να αξιολογείται από διαπιστευμένο ΟΑΣ) με τις προδιαγραφές ασφάλειας (Security Target) που έχει ορίσει ο κατασκευαστής του συστήματος προκειμένου να διατηρεί την αξιολόγηση και τον χαρακτηρισμό «ΕΑΑΔΥ». Προαιρετικά, ο φορέας αυτός να συμμορφώνεται (και να αξιολογείται από διαπιστευμένο ΟΑΣ), με το πρότυπο ETSI EN 319 401.

9.3. Μετά την επιτυχή ολοκλήρωση του ελέγχου του ΠΥΕ, ο ΟΑΣ εκδίδει Έκθεση Αξιολόγησης Συμμόρφωσης (ΕΑΣ). Αυτή είναι μία λεπτομερής αναφορά που περιέχει όλα τα αποτελέσματα της αξιολόγησης που έχει εκτελεστεί και παρέχεται στον ελεγχόμενο Πάροχο Υπηρεσιών Εμπιστοσύνης (ΠΥΕ). Ακολούθως, ο Πάροχος υποβάλει υποχρεωτικά εντός τριών (3) εργάσιμων ημερών την ΕΑΣ στην ΕΕΤΤ. Μετά από πλήρη έλεγχο και αξιολόγηση της ΕΑΣ, η ΕΕΤΤ αποφασίζει εάν ο Πάροχος και οι αντίστοιχες υπηρεσίες εμπιστοσύνης που παρέχει συμμορφώνονται με τις απαιτήσεις που ορίζει ο Κανονισμός eIDAS. Εντός τριών (3) μηνών μετά την υποβολή της ΕΑΣ, ο Πάροχος ενημερώνεται από την ΕΕΤΤ με σχετική επιστολή για το αποτέλεσμα του ελέγχου συμμόρφωσης. Εάν αυτό είναι θετικό, η/οι ελεγχόμενη/ες υπηρεσία/ες εμπιστοσύνης λαμβάνει/ουν την κατάσταση "εγκεκριμένη" (status “granted”) και προστίθενται στον Εθνικό Κατάλογο Εμπιστοσύνης από την ΕΕΤΤ, εάν δεν περιλαμβάνονται ήδη σε αυτόν. Σε περίπτωση που το αποτέλεσμα του ελέγχου είναι αρνητικό, δηλαδή ο Πάροχος και οι υπηρεσίες εμπιστοσύνης που παρέχει δεν πληρούν τις απαιτήσεις που ορίζονται στον Κανονισμό eIDAS, η ΕΕΤΤ δεν δίδει την κατάσταση "εγκεκριμένη" για τις ελεγχόμενες υπηρεσίες εμπιστοσύνης και ενημερώνει αναλόγως τον Εθνικό Κατάλογο Εμπιστοσύνης.

9.4. Ο σκοπός της ΕΑΣ δεν είναι να επιβεβαιώσει ότι ο Πάροχος και οι υπηρεσίες που παρέχει είναι σύμφωνα με συγκεκριμένα τεχνικά πρότυπα, αλλά ότι είναι σε συμμόρφωση με τον Κανονισμό eIDAS. Η συμμόρφωση με τεχνικά πρότυπα σε κάποιες περιπτώσεις υπονοεί τη συμμόρφωση με κάποιες απαιτήσεις του Κανονισμού eIDAS, οπότε δεν είναι υποχρεωτική. Συστήνεται η ~~παρακολούθηση~~ συμμόρφωση των Παρόχων με τα σχετικά~~των~~ ~~ε~~Ευρωπαϊκ~~ών~~ά προ~~θ~~τύ~~υ~~π~~ων~~α (ETSI, European Telecommunications Standards Institute και CEN, European Committee for Standardisation) για να εξασφαλιστεί η διαλειτουργικότητα των υπηρεσιών που παρέχουν οι εγκεκριμένοι ~~Πάροχοι~~ΠΥΕ.

9.5. Ο ~~Πάροχος~~ ΠΥΕ μπορεί να ενεργοποιήσει την εγκεκριμένη υπηρεσία μόνο εφόσον ενταχθεί στον Εθνικό Κατάλογο Εμπιστοσύνης, όπως προβλέπεται στο Άρθρο 22 του Κανονισμού eIDAS.

Άρθρο 10

Περιεχόμενα της ΕΑΣ και κριτήρια αξιολόγησης του παρόχου υπηρεσιών εμπιστοσύνης

Η ΕΑΣ πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα στοιχεία, με την επιφύλαξη ότι η ΕΕΤΤ μπορεί να ζητήσει πρόσθετες πληροφορίες από τον Πάροχο (ΠΥΕ):

1. Στοιχεία του ΟΑΣ, συμπεριλαμβανομένων, της στοιχείων εγγραφής σε δημόσια αρχεία, την έδρα του και τα δεδομένα επικοινωνίας (αριθμός τηλεφώνου και διεύθυνση ηλεκτρονικού ταχυδρομείου του νομίμου εκπροσώπου).
2. Στοιχεία του Φορέα Διαπίστευσης που έχει διαπιστεύσει τον ΟΑΣ (ταχυδρομική διεύθυνση και e-mail) καθώς και πληροφορίες που αφορούν το πιστοποιητικό διαπίστευσης (π.χ. αριθμό αναγνώρισης του πιστοποιητικού).
3. Το πιστοποιητικό του ΟΑΣ, που έχει εκδοθεί από τον Φορέα Διαπίστευσης και λεπτομερή περιγραφή του συστήματος διαπίστευσης που χρησιμοποιήθηκε, συμπεριλαμβανομένης της δήλωσης συμμόρφωση με τις απαιτήσεις του κανονισμού eIDAS, ιδίως διαπίστευση σύμφωνα με το πρότυπο ISO / IEC 17065 πρότυπο και ETSI EN 319 403 για την αξιολόγηση της συμμόρφωσης των παρόχων και των υπηρεσιών.
4. Στοιχεία του αρμόδιου της ΕΑΣ.

Με σχόλια [DZ50]: Δεν είναι κατανοητός ο λόγος που υπάρχει αυτή η προθεσμία. Ο Πάροχος είναι υποχρεωμένος να καταθέσει την έκθεση συμμόρφωσης πριν τη λήξη των 24 μηνών. Επίσης, επειδή η διαδικασία Πιστοποίησης είναι αρκετά χρονοβόρα και με υψηλό κόστος, οι Πάροχοι συνήθως σχεδιάζουν την επιθεώρηση κοντά στο τέλος του διαστήματος εγκυρότητας του Πιστοποιητικού. Σύμφωνα με τις διεθνείς πρακτικές, προβλέπεται ένα διάστημα «παράτασης» μέχρι να κατατεθεί η νέα Πιστοποίηση στον Φορέα Ελέγχου. Συνεπώς, θα μπορούσε να δοθεί ένα περιθώριο στους Παρόχους να καταθέσουν την έκθεση συμμόρφωσης στην ΕΕΤΤ το αργότερο εντός τριών (3) μηνών από την ημερομηνία λήξης της προηγούμενης Πιστοποίησης, όπως ισχύει στα μεγαλύτερα διεθνή “Trust Store” προγράμματα (πχ Microsoft, Mozilla).

Με σχόλια [DZ51]: Δεν προσδιορίζεται ποια είναι η «κατάλληλη» ενημέρωση. Υπάρχει λόγος να αναφερθεί η κατάσταση “withdrawn” κατ’ αναλογία με την παραπάνω αναφορά του status “granted”?

Με σχόλια [DZ52]: Δεν είναι κατανοητή η συγκεκριμένη διατύπωση. Αν καταλαβαίνουμε σωστά το νόημα της πρότασης, θα μπορούσε να επαναδιατυπωθεί ως εξής:
«Υπάρχουν συγκεκριμένα τεχνικά πρότυπα του οργανισμού ETSI (European Telecommunications Standards Institute)
-ETSI EN 319 401
-ETSI EN 319 411-1
-ETSI EN 319 411-2
-ETSI EN 319 421
και CEN (European Committee for Standardization) στα παραρτήματα των οποίων γίνονται αναφορές συσχέτισης με τον Κανονισμό eIDAS χωρίς όμως ο Κανονισμός eIDAS, έως την έναρξη ισχύος του παρόντος κανονισμού, να υποχρεώνει την εφαρμογή των συγκεκριμένων τεχνικών προτύπων».

Με σχόλια [DZ53]: Μέχρι σήμερα, δεν υπάρχουν παραδείγματα Διαπίστευσης ΟΑΣ μόνο ως προς τις απαιτήσεις του κανονισμού eIDAS, χωρίς να αναφέρουν Διαπίστευση στο πρότυπο ISO/IEC 17065 ή το ETSI EN 319 403. Παρακαλούμε συμβουλευθείτε το https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation. Προτείνουμε να υπάρχει υποχρεωτικά Διαπίστευση του ΕΑΣ σύμφωνα με:
- τον Κανονισμό eIDAS ΚΑΙ ISO/IEC 17065 ή
- τον Κανονισμό eIDAS ΚΑΙ ETSI EN 319 403

5. Στοιχεία του Παρόχου, συμπεριλαμβανομένων του ονόματός, τον αριθμό μητρώου και την ταχυδρομική διεύθυνση, όπως αναφέρονται σε επίσημα αρχεία, και το e-mail
6. Αναλυτική λίστα των εγκεκριμένων υπηρεσιών, για τις οποίες ο ΟΑΣ επιβεβαιώνει ότι πληρούν τις απαιτήσεις του ~~Κανονισμός~~ Κανονισμού eIDAS. Οι υπηρεσίες καταγράφονται με 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. Επίσης περιλαμβάνει το αναγνωριστικό κλειδιού, σύμφωνα με το πρότυπο RFC 5280 ή το δημόσιο κλειδί της υπηρεσίας, και το πιστοποιητικό X.509 V3 που αυτή χρησιμοποιεί στη μορφή Base64 PEM.
7. Για κάθε υπηρεσία της λίστας υπό 6, περιγραφή της φυσικής, λογικής και λειτουργικής αρχιτεκτονικής.
8. Κατάλογο των πιστοποιήσεων για την υπό εξέταση υπηρεσία ή προϊόν που χρησιμοποιεί ο Πάροχος, συμπεριλαμβανομένου ενός αντιγράφου ή συνδέσμου (link) σε αυτές. Στην περίπτωση εγκεκριμένης συσκευής δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας, επισυνάπτεται αντίγραφο ή σύνδεσμος της πιστοποίησης που έχει εκδοθεί από τον Φορέα Διαπίστευσης, όπου συγκεκριμένα αναφέρονται τα χαρακτηριστικά της συσκευής και η υπηρεσία ή οι υπηρεσίες που τη χρησιμοποιούν.
9. Σε περίπτωση που ο Π~~π~~άροχος παρέχει προηγμένη ή απομακρυσμένη υπηρεσία ηλεκτρονικής υπογραφής, προσκομίζεται τεκμηρίωση των διαδικασιών που ακολουθούνται, των μηχανισμών διαχείρισης ασφάλειας, των αξιόπιστων συστημάτων και προϊόντων που χρησιμοποιούνται, συμπεριλαμβανομένων 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.
10. ~~Σε περίπτωση που ο πάροχος παρέχει προηγμένη ή απομακρυσμένη υπηρεσία ηλεκτρονικής σφραγίδας, προσκομίζεται τεκμηρίωση των διαδικασιών που ακολουθούνται, των μηχανισμών διαχείρισης ασφάλειας, των αξιόπιστων συστημάτων και προϊόντων που χρησιμοποιούνται, συμπεριλαμβανομένων ασφαλών διαύλων ηλεκτρονικής επικοινωνίας για τη διασφάλιση ότι το περιβάλλον της ηλεκτρονικής σφραγίδας είναι αξιόπιστο και ότι ο υπογράφων έχει υψηλό επίπεδο εμπιστοσύνης και τον αποκλειστικό έλεγχο της χρήσης δεδομένων δημιουργίας ηλεκτρονικής σφραγίδας.~~
11. 10. Λεπτομερή κατάλογο όλων των εγγράφων του παρόχου, δημόσιων και εσωτερικών. Επιπλέον, θα πρέπει να υπάρχει τεκμηρίωση δημοσίως διαθέσιμη ή αναφορά των διαθέσιμων συνδέσμων (links) σε αυτή. Η τεκμηρίωση πρέπει να περιλαμβάνει τουλάχιστον:
    - ~~11.1.~~10.1. Δήλωση των πρακτικών υπηρεσίας εμπιστοσύνης.
    - ~~11.2.~~10.2. Πολιτικές κάθε υπηρεσίας εμπιστοσύνης.
    - ~~11.3.~~10.3. Σχέδιο παύσης δραστηριοτήτων που αναφέρεται στο άρθρο 24 παράγραφος 2 σημείο (~~i~~η) του κανονισμού eIDAS.
    - ~~11.4.~~10.4. Σύμβαση αιτήματος παροχής υπηρεσιών και όροι χρήσης.
12. 11. Η ΕΑΣ θα πρέπει να προσδιορίζει το χρονικό διάστημα που αφορά ο έλεγχος, τους πόρους που χρησιμοποιήθηκαν, καθώς και την εργασία κάθε ελεγκτή.
13. 12. Για καθεμία από τις ακόλουθες απαιτήσεις του Κανονισμού eIDAS, πρέπει να αναγράφεται στην ΕΑΣ ο τρόπος συμμόρφωσης του παρόχου, καθώς και μια λίστα με τα σημεία ελέγχου και στόχων που χρησιμοποιούνται στον έλεγχο, διευκρινίζοντας κατά περίπτωση τις αδυναμίες συμμόρφωσης και το επίπεδο συνάφειας:
    - ~~13.1.~~12.1. Γενικές απαιτήσεις που καθορίζονται στον κανονισμό για τους παρόχους και τις υπηρεσίες:
        - ~~13.1.1.~~12.1.1. Ευθύνη και βάρος αποδείξεως (άρθρο 13), και ειδικότερα:

Με σχόλια [DZ54]: Προτείνεται να προστεθεί το κείμενο «… για τη συμμόρφωση του Παρόχου στις προδιαγραφές ασφάλειας (Security Target) που έχει ορίσει η αξιολόγηση του συστήματος απομακρυσμένης υπογραφής, προκειμένου να θεωρείται «Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής».» Επιπλέον, αυτή η τεκμηρίωση είναι εμπιστευτική, είναι στη διάθεση του ΟΑΣ (που δεσμεύεται από σύμβαση εχεμύθειας). Δεν προβλέπεται από τον Κανονισμό ή άλλη διάταξη η προσκόμιση της συγκεκριμένης τεκμηρίωσης στην Εποπτική Αρχή. Προτείνεται να τροποποιηθεί η απαίτηση και να προσκομίζεται από τον Πάροχο βεβαίωση ή Πιστοποίηση από τον ΟΑΣ ότι ακολουθούνται πολιτικές και διαδικασίες σύμφωνα με τις προδιαγραφές ασφάλειας (Security Target) που έχει ορίσει ο κατασκευαστής του συστήματος προκειμένου να διατηρεί την αξιολόγηση και τον χαρακτηρισμό «Εγκεκριμένης Διάταξης Δημιουργίας Υπογραφής».

Με σχόλια [DZ55]: Υπερβολική απαίτηση. Η ανακοίνωση και μόνο ύπαρξης συγκεκριμένων εσωτερικών αρχείων, θέτει ζήτημα ασφάλειας των Παρόχων. Ο κατάλογος και τα ίδια τα έγγραφα του Παρόχου, είναι στη διάθεση των ΟΑΣ κατά τη διαδικασία επιθεώρησης. Ο ΟΑΣ δεσμεύεται με σύμβαση εχεμύθειας προκειμένου να μην υπάρξει διαρροή των εγγράφων ή ακόμα και της πληροφορίας ύπαρξης συγκεκριμένων εγγράφων.

Με σχόλια [DZ56]: Το λεπτομερές σχέδιο εξακολουθεί να παραμένει εμπιστευτικό για τον Πάροχο. Μια περίληψη του σχεδίου συνήθως δημοσιεύεται στο CP/CPS.

i. Όρια ευθύνης.
ii. Όρια όσον αφορά τις πιθανές χρήσεις των υπηρεσιών, συμπεριλαμβανομένης της επιβολής ορίων αποζημίωσης της υπερβολικής χρήση τους.

~~13.1.2.~~12.1.2. Προσβασιμότητα για άτομα με αναπηρίες (Άρθρο 15)

~~13.1.3.~~12.1.3. Απαιτήσεις ασφάλειας για τους παρόχους υπηρεσιών εμπιστοσύνης (Άρθρο 19)

~~13.1.4.~~12.1.4. Απαιτήσεις για τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης (Άρθρο 24)

~~13.2.~~12.2. Ειδικές απαιτήσεις που καθορίζονται στον κανονισμό για τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης:

~~13.2.1.~~12.2.1. Δημιουργία εγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής

Άρθρο 28: Εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών

Άρθρο 29: Απαιτήσεις για τις εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής υπογραφής

~~13.2.2.~~12.2.2. Δημιουργία εγκεκριμένου πιστοποιητικού ηλεκτρονικής σφραγίδας

~~13.2.3.~~12.2.3. Άρθρο 38: Εγκεκριμένα πιστοποιητικά ηλεκτρονικής σφραγίδας

Άρθρο 39: Εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής σφραγίδας

~~13.2.4.~~12.2.4. Δημιουργία εγκεκριμένου πιστοποιητικού ηλεκτρονικής χρονοσφραγίδας

Άρθρο 42: Απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές χρονοσφραγίδες

~~13.2.5.~~12.2.5. Επικύρωση εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων

Άρθρο 32 (40): Απαιτήσεις για την επικύρωση εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων

Άρθρο 33 (40): Εγκεκριμένη υπηρεσία επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων

~~13.2.6.~~12.2.6. Διαφύλαξη εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων

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

~~13.2.7.~~12.2.7. Εγκεκριμένη υπηρεσία συστημένης παράδοσης

Άρθρο 44: Απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές υπηρεσίες συστημένης παράδοσης

~~13.2.8.~~12.2.8. Δημιουργία εγκεκριμένου πιστοποιητικού πιστοποίησης γνησιότητας ιστοτόπων

Άρθρο 45: Απαιτήσεις για εγκεκριμένα πιστοποιητικά γνησιότητας ιστότοπου

~~14.~~13. Όταν η συμμόρφωση αξιολογείται περαιτέρω, σύμφωνα με συγκεκριμένο πρότυπο (ευρωπαϊκά πρότυπα ETSI EN 319 401 / ETSI EN 319 411-1 / ETSI EN 319 411-2 / ETSI EN 319 421), η ΕΑΣ περιλαμβάνει ξεχωριστή αναφορά με ρητή ένδειξη των μη συμμορφώσεων και της συνάφειάς τους.

~~15.~~14. Η ΕΑΣ αναφέρει λεπτομερώς τον κατάλογο των τρίτων μερών στους οποίους έχουν εξουσιοδοτηθεί πλήρως ή μερικώς διαδικασίες παροχής υπηρεσιών εμπιστοσύνης.

~~16.~~15. Η ΕΑΣ αναφέρει το χρονοδιάγραμμα ελέγχου.

~~17.~~16. Η ΕΑΣ αναφέρει τυχόν απαιτούμενους προγραμματισμένους επιπλέον ελέγχους που πρόκειται να πραγματοποιήσει ο ΟΑΣ.

~~18.~~17. Σύνοψη με τα σημεία τα οποία δεν υπάρχει συμμόρφωση.

~~19.~~18. Πιθανές συστάσεις προς τον πάροχο.

Με σχόλια [DZ57]: Συνήθως πρόκειται για προτάσεις βελτίωσης και είναι πολλές φορές αρκετά υποκειμενικές χωρίς να επηρεάζουν κρίσιμα σημεία των διαδικασιών και τη συνολική συμμόρφωση. Δεν έχουν δημόσιο ενδιαφέρον για να κοινοποιούνται εκτός του Παρόχου και θα προκαλέσουν περισσότερο παρεξηγήσεις και σύγχιση. Προτείνουμε την αφαίρεση της απαίτησης.

Άρθρο 11

Ανάκληση εγκεκριμένων πιστοποιητικών για ψηφιακές υπογραφές ή ηλεκτρονικές σφραγίδες

1. Ο ΠΥΕ υποχρεούται να προβεί σε άμεση ανάκληση ενός εγκεκριμένου πιστοποιητικού, στις εξής περιπτώσεις:
   α. μετά από αίτηση του ~~δικαιούχου~~ κατόχου/συνδρομητή του πιστοποιητικού ή του νομίμως εξουσιοδοτημένου από αυτόν ατόμου
   β. εφόσον διαπιστωθεί από την ΕΕΤΤ, στα πλαίσια της εποπτικής και ελεγκτικής της αρμοδιότητας, ότι το εγκεκριμένο πιστοποιητικό περιέχει ψευδείς ή ανακριβείς πληροφορίες ως προς τις απαιτήσεις του Κανονισμού eIDAS
   γ. σε περίπτωση πιστοποιητικού η έκδοση του οποίου βασίστηκε σε ψευδείς ή ανακριβείς πληροφορίες
   δ. σε περίπτωση τερματισμού εργασιών του ΠΥΕ, σύμφωνα με το Άρθρο 7 της παρούσας,
   ε. σε περίπτωση απώλειας της δικαιοπρακτικής ικανότητας, κήρυξης σε αφάνεια ή σε περίπτωση θανάτου του κατόχου/συνδρομητή ~~δικαιούχου~~ του πιστοποιητικού, λαμβάνοντας υπόψη ότι κάθε πιστοποιητικό δημιουργίας ηλεκτρονικής υπογραφής είναι αμεταβίβαστο σε κάθε περίπτωση
   στ. σε περίπτωση που τελεσίδικη δικαστική απόφαση διατάσσει την σχετική ανάκληση ή ακύρωση
   ζ. αν από την μεταξύ ΠΥΕ και κατόχου/συνδρομητή ~~δικαιούχου~~ σύμβαση απορρέει σχετική προς τούτο υποχρέωση ή/και δικαίωμα, ενός των συμβαλλομένων μερών. Στην περίπτωση αυτή, αν το αίτημα για ανάκληση τεθεί από τον κάτοχο/συνδρομητή ~~δικαιούχο~~ πιστοποιητικού, ο ΠΥΕ υποχρεούται να προβεί σε άμεση ανάκληση, δικαιούμενος να επιφυλαχθεί για κάθε νόμιμο ή συμβατικό του δικαίωμα
   η. σε περίπτωση που υπάρχουν αποχρώσες ενδείξεις ότι τα δεδομένα δημιουργίας υπογραφής/σφραγίδας του κατόχου/συνδρομητή ~~δικαιούχου~~ του πιστοποιητικού έχουν γίνει γνωστά ή/και χρησιμοποιούνται από τρίτους
   θ. σε περίπτωση κατά την οποία ~~τα δεδομένα δημιουργίας υπογραφής/σφραγίδας~~κάποιο ιδιωτικό κλειδί Αρχής Πιστοποίησης του ΠΥΕ έχουν γίνει γνωστά σε τρίτους
   ι. σε περίπτωση κατά την οποία ο κάτοχος/συνδρομητής ~~δικαιούχος~~ πιστοποιητικού, το οποίο χρησιμοποιεί με συγκεκριμένη ιδιότητα, απωλέσει την ιδιότητα αυτή (ενδεικτικά, σε περίπτωση αποχώρησης εργαζομένου στον οποίο έχει εκδοθεί τέτοιο πιστοποιητικό με την ιδιότητα ως υπαλλήλου συγκεκριμένης υπηρεσίας ή θέσης) ή σε κάθε περίπτωση κατά την οποία στοιχεία που περιλαμβάνονται στο πιστοποιητικό τροποποιηθούν.
2. Πιστοποιητικό που έχει ανακληθεί δεν είναι δυνατόν να επανατεθεί σε ισχύ.
3. Ο ΠΥΕ δικαιούται, μέχρι την εξακρίβωση και επιβεβαίωση ή όχι των λόγων ανάκλησης πιστοποιητικού, να προβεί σε άμεση αναστολή του.
4. Αν ένα εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής/σφραγίδας τεθεί προσωρινά σε αναστολή, το πιστοποιητικό χάνει την εγκυρότητά του όσο βρίσκεται σε κατάσταση αναστολής. Η περίοδος αναστολής δεν μπορεί να υπερβαίνει τις δύο (2) εβδομάδες.

Με σχόλια [DZ58]: Η συγκεκριμένη διάταξη ισχύει μόνο για Εγκεκριμένα Πιστοποιητικά για Ηλεκτρονικές Υπογραφές. Δεν ισχύει για την περίπτωση των Εγκεκριμένων Πιστοποιητικών για Ηλεκτρονικές Σφραγίδες όπου ο νόμιμος εκπρόσωπος έχει τον έλεγχο του αντίστοιχου ιδιωτικού κλειδιού, το οποίο θα μπορούσε να μεταβιβάζεται.

Με σχόλια [DZ59]: Δεν πιστοποιείται ούτε ελέγχεται η συγκεκριμένη απαίτηση. Προτείνεται αναδιατύπωση «σε περίπτωση που ο Πάροχος διαπιστώσει ότι τα δεδομένα δημιουργίας υπογραφής/σφραγίδας του κατόχου/συνδρομητή του Πιστοποιητικού έχουν γίνει γνωστά ή/και χρησιμοποιούνται από τρίτους»

5. Ο ΠΥΕ πρέπει να καταχωρήσει την περίοδο αναστολής στο αρχείο του πιστοποιητικού και να έχει διαθέσιμη στο κοινό την πληροφορία για την κατάσταση αναστολής του πιστοποιητικού για όλη την διάρκεια αναστολής.
6. Σε κάθε περίπτωση, ο ΠΥΕ πρέπει να ενημερώσει αμέσως τους ~~δικαιούχους~~ κατόχους/συνδρομητές πιστοποιητικών για την αναστολή/ανάκληση των τελευταίων και να είναι σε θέση να αποδείξει ότι τους έχει ενημερώσει.
7. Ο ΠΥΕ εγκεκριμένων πιστοποιητικών παρέχει υπηρεσία ανάκλησης πιστοποιητικών, η οποία λειτουργεί αδιαλείπτως επί 24 ώρες την ημέρα και επί 7 ημέρες την εβδομάδα, συμπεριλαμβανομένων αργιών, στην οποία οι κάτοχοι εγκεκριμένων πιστοποιητικών ή/και τα νομίμως εξουσιοδοτημένα από αυτούς πρόσωπα, δύνανται να υποβάλουν αίτημα ανάκλησης, σύμφωνα με την παράγραφο 1α του παρόντος άρθρου. Σε κάθε περίπτωση, πριν από την ανάκληση, ο ΠΥΕ επαληθεύει ότι το αίτημα υποβάλλεται από πρόσωπο που νομιμοποιείται προς τούτο.
8. Οι αιτήσεις ανάκλησης εγκεκριμένων πιστοποιητικών πρέπει να τυγχάνουν άμεσης επεξεργασίας (εντός 24ώρου).
9. Ο ΠΥΕ εγκεκριμένων πιστοποιητικών υποχρεούται να διασφαλίζει ότι τα αιτήματα για ανάκληση μπορούν να γίνουν και τηλεφωνικά και υποχρεώνεται να ενημερώνει τους ~~δικαιούχους~~ κατόχους/συνδρομητές των πιστοποιητικών για αυτό, γνωστοποιώντας τους το σχετικό αριθμό τηλεφώνου.
10. Ο ΠΥΕ εγκεκριμένων πιστοποιητικών παρέχει υπηρεσία ενημέρωσης σχετικά με την κατάσταση (ισχύ, ανάκληση) των πιστοποιητικών, η οποία λειτουργεί αδιαλείπτως επί 24 ώρες την ημέρα και επί 7 ημέρες την εβδομάδα συμπεριλαμβανομένων αργιών. Ο ΠΥΕ θα πρέπει να διασφαλίσει την ακεραιότητα και αυθεντικότητα της πληροφορίας σχετικά με την κατάσταση των πιστοποιητικών και την διαθεσιμότητά της σε διεθνές επίπεδο.
11. Εφόσον ο ΠΥΕ εγκεκριμένων πιστοποιητικών παρέχει την υπηρεσία της παραγράφου 8 με τη διατήρηση λίστας ανακληθέντων πιστοποιητικών, στην οποία εγγράφει τα ανακληθέντα ή υπό αναστολή πιστοποιητικά, η λίστα αυτή υποχρεωτικά :
    α. εκδίδεται, κατ' ελάχιστον, μία φορά ημερησίως,
    β. αναγράφει την ώρα της επόμενης ενημέρωσής της,
    γ. είναι δυνατόν να ενημερώνεται πριν από την, υπό στοιχείο β΄, ώρα επόμενης ενημέρωσής της,
    δ. περιλαμβάνει, κατ' ελάχιστον, την ημερομηνία, το χρόνο της ανάκλησης, την κατάσταση του πιστοποιητικού (σε αναστολή ή ανάκληση) και ~~τον~~ ένα μοναδικό ~~κωδικό~~ σειριακό αριθμό ταυτοποίησης του πιστοποιητικού,
    ε. είναι προσπελάσιμη ατελώς από τους ~~δικαιούχους~~ κατόχους/συνδρομητές πιστοποιητικών ή τρίτους.

Άρθρο 12

Υποχρέωση Τήρησης Αρχείου εγκεκριμένων πιστοποιητικών για ηλεκτρονικές υπογραφές ή ηλεκτρονικές σφραγίδες

12.1. Κάθε ΠΥΕ τηρεί τουλάχιστον σε ηλεκτρονική μορφή Αρχείο με το σύνολο των πληροφοριών σχετικά με τα εγκεκριμένα πιστοποιητικά που εκδίδει ή/και διαχειρίζεται, και ιδίως στοιχεία για τον χρόνο έκδοσης, ακύρωσης ή αναστολής και λήξης αυτών προκειμένου να καθίσταται δυνατή η επιβεβαίωση της ορθότητας και της ακρίβειάς τους.

Με σχόλια [DZ60]: Δεν είναι σαφές ποιο είναι αυτό το αρχείο.

Με σχόλια [DZ61]: Η επεξεργασία δεν συνεπάγεται και την άμεση ανάκληση του εγκεκριμένου Πιστοποιητικού. Υπάρχουν περιπτώσεις που απαιτείται διερεύνηση που χρειάζεται περισσότερο χρόνο. Να διευκρινιστεί τι εννοείται με το «άμεσης επεξεργασίας». Αρκεί να υπάρξει μια απάντηση στο αίτημα ανάκλησης που να αναφέρει ότι «εξετάζουμε το αίτημά σας» ή θα πρέπει να έχει ολοκληρωθεί η διερεύνηση και να υπάρχει απόφαση για ανάκληση ή όχι μέσα σε 24 ώρες; Το δεύτερο είναι επικίνδυνο και αρκετά δύσκολο να εφαρμοστεί στην πράξη.

Με σχόλια [DZ62]: Θεωρούμε ότι η συγκεκριμένη απαίτηση είναι υπερβολική. Μπορεί ένας πάροχος να μην επιθυμεί να παρέχει τηλεφωνική εξυπηρέτηση για τα συγκεκριμένα αιτήματα. Η Διεθνής πρακτική δεν επιβάλλει τη χρήση τηλεφώνου. Επιπλέον, μέσω τηλεφώνου δεν διασφαλίζεται ότι η επικοινωνία γίνεται με τον πραγματικό κάτοχο/συνδρομητή. Προτείνεται να αλλάξει η διάταξη από υποχρεωτική σε προαιρετική.

Με σχόλια [DZ63]: Μόνο για τα Εγκεκριμένα Πιστοποιητικά θα υπάρχει πρόβλεψη; Στις υπηρεσίες Συστημένης Παράδοσης ή Χρονοσήμανσης δεν υπάρχει υποχρέωση τήρησης αρχείου και μεταβίβασής του;

12.2. Κάθε εγκεκριμένο πιστοποιητικό, αμέσως μετά την έκδοσή του, καταχωρείται σε ηλεκτρονική μορφή στο Αρχείο, κατά τρόπο ώστε να καθίσταται δυνατός ο εντοπισμός οποιασδήποτε μεταγενέστερης αλλοίωσής του. Η ΕΕΤΤ δύναται με απόφασή της να ρυθμίσει τη διαδικασία που αφορά τον εντοπισμό τέτοιας αλλοίωσης. Η ΕΕΤΤ δύναται με απόφασή της να ρυθμίζει τα σχετικά με τη διαχείριση του Αρχείου των ΠΥΕ.

12.3. Ο ΠΥΕ παρέχει στον κατόχο/συνδρομητή ~~δικαιούχο~~ του εγκεκριμένου πιστοποιητικού πρόσβαση στα δεδομένα που τον αφορούν, κατόπιν υποβολής σχετικού αιτήματός του, στο οποίο ο ΠΥΕ υποχρεούται να απαντήσει εντός αποκλειστικής προθεσμίας επτά (7) ημερών από την ημερομηνία υποβολής του αιτήματος.

12.4. Κατόπιν αιτήματος ή εντολής δικαστικών ή άλλων αρμόδιων Αρχών, ο ΠΥΕ οφείλει να παρέχει πρόσβαση στο έντυπο ή/και ηλεκτρονικό αρχείο σύμφωνα με το Άρθρο 24(2)(η) του Κανονισμού eIDAS.

12.5. Σε περίπτωση εγκεκριμένου πιστοποιητικού για το οποίο χρησιμοποιείται ψευδώνυμο, ο ΠΥΕ υποχρεούται να γνωστοποιεί τα δεδομένα που αφορούν την ταυτότητα του κατόχου/συνδρομητή ~~δικαιούχου~~ του εγκεκριμένου πιστοποιητικού σε τρίτο μέρος, αν το τρίτο μέρος έχει αποδεδειγμένα υπερισχύον νόμιμο συμφέρον για να λάβει γνώση των στοιχείων ταυτότητας του κατόχου/συνδρομητή~~δικαιούχου~~. Ο ΠΥΕ έχει υποχρέωση να καταγράψει την εν λόγω γνωστοποίηση των δεδομένων και να ενημερώσει σχετικά τον κάτοχο/συνδρομητή ~~δικαιούχο~~ του εγκεκριμένου πιστοποιητικού.

12.6. Κάθε καταχώρηση εγκεκριμένου πιστοποιητικού διατηρείται στο Αρχείο για χρονική περίοδο τουλάχιστον επτά (7) ετών από τη λήξη ισχύος του εγκεκριμένου πιστοποιητικού, ελλείψει τέτοιας πληροφορίας, επτά (7) έτη από την ημερομηνία εμφάνισης των πληροφοριών σχετικά με τα δεδομένα που έχουν εκδοθεί και ληφθεί από τον ΠΥΕ στο πλαίσιο των δραστηριοτήτων του.

Με σχόλια [DZ64]: Πώς θα υπάρχει έλλειψη τέτοιας πληροφορίας; Τα ψηφιακά πιστοποιητικά έχουν ημερομηνία λήξης (validTo) τα οποία σύμφωνα με το 12.1 οφείλει ο ΠΥΕ να τα διατηρεί σε ηλεκτρονική μορφή. Προτείνεται να αφαιρεθεί το κείμενο από το «ελλείψει τέτοιας πληροφορίας» μέχρι τέλος της πρότασης.

Μέρος Δ' : Εποπτεία, Τελικές διατάξεις

Άρθρο 13
Εποπτεία και κυρώσεις

Η ΕΕΤΤ εποπτεύει τους εγκατεστημένους στην Ελλάδα παρόχους υπηρεσιών εμπιστοσύνης ως προς την τήρηση των απαιτήσεων και των υποχρεώσεων που θεσπίζει ο Κανονισμός (ΕΕ) 910/2014 (eIDAS) και ο παρών Κανονισμός ΕΕΤΤ. Προς το σκοπό αυτό διενεργεί τις εποπτικές δραστηριότητες που προβλέπονται στον Κανονισμό (ΕΕ) 910/2014 (eIDAS) και σε περίπτωση διαπίστωσης παραβάσεων δύναται, ύστερα από προηγούμενη ακρόαση των ενδιαφερομένων, να επιβάλει τις διοικητικές κυρώσεις που προβλέπονται στο άρθρο 77 παρ. 3 του Ν. 4070/2012.

Άρθρο 14
Μεταβατικές διατάξεις

Από τη θέση σε ισχύ του παρόντος Κανονισμού καταργείται η Απόφαση ΕΕΤΤ 248/71/15.3.2002 «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής

Υπογραφής» (ΦΕΚ 603 Β/16-5-2002), καθώς και η απόφαση ΑΠ 775/5/1-9-16 (ΦΕΚ 3156/Β/30-9-16) περί τροποποίησης του εν λόγω Κανονισμού.

Εγκεκριμένα πιστοποιητικά που εκδίδονται για φυσικά πρόσωπα σύμφωνα με την Οδηγία 1999/93/ΕΚ θεωρούνται εγκεκριμένα πιστοποιητικά για τις ηλεκτρονικές υπογραφές βάσει του Κανονισμού eIDAS μέχρι την ημερομηνία λήξης τους, εφόσον ο εγκεκριμένος ΠΥΕ υποβάλει έκθεση αξιολόγησης της συμμόρφωσης στην ΕΕΤΤ για την υπηρεσία αυτή σύμφωνα με τα οριζόμενα στο Άρθρο 9 της παρούσας.

Με σχόλια [DZ65]: Φαίνεται αρκετά γενική η συγκεκριμένη περιγραφή, ειδικά αν αναφερόμαστε στην υπηρεσία έκδοσης Πιστοποιητικών για Ψηφιακές Υπογραφές. Αν για παράδειγμα ένας Πάροχος είχε μια υποδομή έκδοσης Αναγνωρισμένων Πιστοποιητικών σύμφωνα με την οδηγία 1999/93/ΕΚ η οποία είχε προβλήματα ασφάλειας (πχ διέρρευσε το ιδιωτικό κλειδί μιας subCA) και ο Πάροχος εγκατέστησε νέα υποδομή σύμφωνα με τις προδιαγραφές του Κανονισμού eIDAS και Πιστοποίησε τη συμμόρφωση της νέας υποδομής, χωρίς να πιστοποιήσει την προηγούμενη υποδομή, δεν θα πρέπει να επιτραπεί στα Πιστοποιητικά της προηγούμενης υποδομής να θεωρούνται «εγκεκριμένα» Πιστοποιητικά για ηλεκτρονικές υπογραφές για τον απλούστατο λόγο ότι ο κάτοχος του ιδιωτικού κλειδιού της παλιάς Αρχής Πιστοποίησης θα μπορούσε να εκδίδει ανεξέλεγκτα και με όποια στοιχεία επιθυμεί (ονοματεπώνυμο, ημερομηνίες έκδοσης/λήξης) ψηφιακά πιστοποιητικά για ψηφιακές υπογραφές. Ως ελάχιστη προϋπόθεση για την επέκταση αποδοχής των «Αναγνωρισμένων» Πιστοποιητικών που εκδόθηκαν βάσει του ΠΔ 150/2001, προτείνουμε την αντικατάσταση της διατύπωσης «για την υπηρεσία αυτή» με «για την υπηρεσία δημιουργίας ηλεκτρονικών υπογραφών, βεβαιώνοντας ότι οι διατάξεις του Κανονισμού eIDAS που αφορούν στην τήρηση της ασφάλειας του Αρχείου (άρθρο 12 του παρόντος κανονισμού) και η υπηρεσία ελέγχου εγκυρότητας των Πιστοποιητικών που εκδόθηκαν, εφαρμόζονται πλήρως».
Επιπλέον, θα ήταν προς όφελος της ασφάλειας των Συνδρομητών και των Relying Parties να οριστεί σε Εθνικό επίπεδο μια καταληκτική ημερομηνία ισχύος των «Αναγνωρισμένων Πιστοποιητικών» που εκδόθηκαν βάσει του ΠΔ 150/2001, για παράδειγμα την 1/7/2019. Ο λόγος είναι ότι υπάρχουν σήμερα έγκυρα «Αναγνωρισμένα» πιστοποιητικά με διάρκεια 5 έτη (λήγουν το 2022) τα οποία έχουν εκδοθεί με διαδικασίες που δεν έχουν πιστοποιηθεί από ανεξάρτητους Φορείς Πιστοποίησης και ενδεχομένως δεν καλύπτουν όλες τις διατάξεις του Κανονισμού eIDAS.

ΑΡΘΡΟ 15

Έναρξη ισχύος

Η ισχύς του παρόντος Κανονισμού αρχίζει από τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως

Παράρτημα 1

Παρεχόμενες εγκεκριμένες υπηρεσίες

1. Δημιουργία εγκεκριμένης Ηλεκτρονικής Υπογραφής
2. Δημιουργία εγκεκριμένης Ηλεκτρονικής Σφραγίδας
3. Επικύρωση εγκεκριμένης Ηλεκτρονικής Υπογραφής
4. Επικύρωση εγκεκριμένης Ηλεκτρονικής Σφραγίδας
5. Διαφύλαξη εγκεκριμένης Ηλεκτρονικής Υπογραφής
6. Διαφύλαξη εγκεκριμένης Ηλεκτρονικής Σφραγίδας
7. Δημιουργία εγκεκριμένης Ηλεκτρονικής Χρονοσφραγίδας
8. Υπηρεσία Συστημένης Παράδοσης
9. Πιστοποίηση Γνησιότητας Ιστοτόπων

Με σχόλια [DZ66]: Προτείνεται να συμβαδίζει με τις 6 ομαδοποιημένες υπηρεσίες του eIDAS

Σύμφωνα με τον Κανονισμό, Άρθρο 3 ορισμός 16, ορίζονται συγκεκριμένες «Υπηρεσίες Εμπιστοσύνης»:
1.Δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών υπογραφών (e-Signatures)
2.Δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών σφραγίδων (e-Seals)
3.Δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών χρονοσφραγίδων (Time Stamping)
4.Δημιουργία, εξακρίβωση και επικύρωση πιστοποιητικών για επαλήθευση ταυτότητας ιστοτόπων (Web Site Authentication)
5.Ηλεκτρονικές υπηρεσίες συστημένης παράδοσης (e-Delivery)
6.Ηλεκτρονικές υπηρεσίες διαφύλαξης ηλεκτρονικών υπογραφών, σφραγίδων ή πιστοποιητικών (e-Preservation)

Παράρτημα 2

Παρεχόμενες μη εγκεκριμένες υπηρεσίες

Με σχόλια [DZ67]: Παρομοίως με το Παράρτημα 1

1. Δημιουργία Ηλεκτρονικής Υπογραφής
2. Δημιουργία Ηλεκτρονικής Σφραγίδας
3. Επικύρωση Ηλεκτρονικής Υπογραφής
4. Επικύρωση Ηλεκτρονικής Σφραγίδας
5. Διαφύλαξη Ηλεκτρονικής Υπογραφής
6. Διαφύλαξη Ηλεκτρονικής Σφραγίδας
7. Δημιουργία Ηλεκτρονικής Χρονοσφραγίδας
8. Υπηρεσία Συστημένης Παράδοσης
9. Πιστοποίηση Γνησιότητας Ιστοτόπων

Παράρτημα 3

Αναφορά εκτίμησης κινδύνων και μέτρων αντιμετώπισης των περιστατικών ασφάλειας

Προτείνεται ~~Αυτή θα πρέπει τουλάχιστον~~ να περιλαμβάνει κατ' ελάχιστον τα ακόλουθα:

Α. Μεθοδολογία διαχείρισης κινδύνων

1. Προσδιορισμός περιουσιακών στοιχείων:
   i. Κύρια περιουσιακά στοιχεία όπως στοιχεία ενεργητικού, επιχειρηματικές διαδικασίες
   ii. Υποστηρικτικά στοιχεία όπως λογισμικό, υλικό και δίκτυα, τοποθεσία, προσωπικό
2. Προσδιορισμός απειλών όπως φυσικοί κίνδυνοι, βασικές υπηρεσίες, απειλές που προκαλούνται από τον άνθρωπο, παράγοντες απειλής.
3. Ανάλυση των ευπαθειών:
   i. Κατά τη διαδικασία εγγραφής συνδρομητών: εγγραφή ~~θέματος~~συνδρομητή, έγκριση/εξουσιοδότηση παροχής υπηρεσίας εμπιστοσύνης, αρχείο εγγραφής
   ii. Κατά τη διαδικασία διαχείρισης κλειδιών~~ού~~ του παρόχου υπηρεσιών εμπιστοσύνης: δημιουργία ζευγών κλειδιών, αποθήκευση ζευγών κλειδιών, δημιουργία αντιγράφων ασφαλείας και ανάκτηση, ~~διάδοση~~ παράδοση και δημοσίευση πιστοποιητικού, χρήση ζευγών κλειδιών
   iii. Κατά τη διαδικασία δημιουργίας πιστοποιητικού: παράδοση σε χρήστη, ~~διάδοση~~ δημοσίευση πιστοποιητικού
   iv. Κατά τη διαδικασία διαχείρισης ανάκλησης: διαδικασία διαχείρισης ανάκλησης πιστοποιητικού, ~~διάδοση~~ δημοσίευση της κατάστασης ανάκλησης πιστοποιητικού
   v. Κατά τη διαδικασία επικύρωσης πιστοποιητικού
   vi. Κατά τη διαδικασία δημιουργίας χρονοσφραγίδας
   vii. στα συστήματα πληροφόρησης και επικοινωνίας του παρόχου υπηρεσιών εμπιστοσύνης: εφαρμογές λογισμικού, υλικό, δίκτυα επικοινωνιών, αρχεία ελέγχου συστημάτων
   viii. ό,τι άλλο επηρεάζει τον πάροχο υπηρεσιών εμπιστοσύνης: πολιτικές, επιχειρησιακές διαδικασίες, προσωπικό, εγκαταστάσεις
4. Προσδιορισμός των αναγκαίων / απαιτούμενων ελέγχων και μέτρα ασφαλείας:
   i. κατά τη διαδικασία εγγραφής
   ii. κατά τη διαδικασία διαχείρισης κλειδιών~~ού~~ του παρόχου υπηρεσιών εμπιστοσύνης: δημιουργία ζεύγους κλειδιών, αποθήκευση ζεύγους κλειδιών, δημιουργία αντιγράφων ασφαλείας και ανάκτηση, διάδοση πιστοποιητικού, χρήση ζεύγους κλειδιών
   iii. κατά τη διαδικασία διαχείρισης κλειδιού: δημιουργία του ζεύγους κλειδιών, διαδικασία παροχής ειδικής ~~της~~ κρυπτοσυσκευής
   iv. κατά τη διαδικασία διαχείρισης του πιστοποιητικού: παράδοση του πιστοποιητικού στο χρήστη, ~~διάδοση~~ δημοσίευση πιστοποιητικού, χρήση πιστοποιητικού
   v. κατά τη διαδικασία διαχείρισης ανάκλησης: υπηρεσία διαχείρισης ανάκλησης πιστοποιητικού, υπηρεσία ~~διάδοσης~~ δημοσίευσης κατάστασης ~~κατάργησης~~ ανάκλησης
   vi. κατά τη διαδικασία επικύρωσης
   vii. κατά τη διαδικασίαδημιουργίας χρονοσφραγίδας~~άγισης~~

viii. στα συστήματα πληροφοριών και επικοινωνιών του παρόχου υπηρεσιών εμπιστοσύνης: εφαρμογές λογισμικού, υλικό, δίκτυα επικοινωνίας
ix. στις λειτουργίες του παρόχου υπηρεσιών εμπιστοσύνης: πολιτικές, επιχειρησιακές διαδικασίες, προσωπικό, εγκαταστάσεις

5. Προσδιορισμός των συνεπειών: 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 αποτέλεσμα ανεπιθύμητου περιστατικού. Μπορεί να μετρηθεί από τις συνέπειες που έχει το περιστατικό στην περιουσία του οργανισμού
    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, σχέδιο τερματισμού υπηρεσίας
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 4

Υποβαλλόμενα Στοιχεία κατά την Έναρξη Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης

ΜΕΡΟΣ Α – ΠΛΗΡΟΦΟΡΙΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΝ ΠΑΡΟΧΟ ΥΠΗΡΕΣΙΩΝ ΕΜΠΙΣΤΟΣΥΝΗΣ		
ΔΙΑΚΡΙΚΟΣ ΤΙΤΛΟΣ ΟΡΓΑΝΙΣΜΟΥ (Όπως εμφανίζεται στην επίσημη καταχώρηση)		ΟΡΓΑΝΙΣΜΟΣ
Ιστοσελίδα:		
Διεύθυνση :		
ΠΟΛΗ / Ταχ. ΚΩΔΙΚΟΣ :		
ΧΩΡΑ :		
ΤΗΛΕΦΩΝΟ :	ΦΑΞ :	Email :
ΕΚΠΡΟΣΩΠΟΣ ΕΠΙΚΟΙΝΩΝΙΑΣ :	ΤΗΛΕΦΩΝΟ :	Email :

ΜΕΡΟΣ Β – ΠΛΗΡΟΦΟΡΙΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΝ ΤΥΠΟ ΤΩΝ ΕΓΚΕΚΡΙΜΕΝΩΝ ΥΠΗΡΕΣΙΩΝ ΕΜΠΙΣΤΟΣΥΝΗΣ ΠΟΥ ΠΑΡΕΧΟΝΤΑΙ
Αναλυτικές πληροφορίες για το είδος των Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης θα επισυναφθεί. Εγκεκριμένες Υπηρεσίες Εμπιστοσύνης που παρέχονται (-σημειώστε στο τετραγωνάκι) : ☐ Δημιουργία εγκεκριμένης Ηλεκτρονικής Υπογραφής (Αρθρ. 28 του Κανονισμού eIDAS) ☐ Δημιουργία εγκεκριμένης Ηλεκτρονικής Σφραγίδας (Αρθρ. 38 του Κανονισμού eIDAS) ☐ Επικύρωση εγκεκριμένης Ηλεκτρονικής Υπογραφής (Αρθρ. 33 του Κανονισμού eIDAS) ☐ Επικύρωση εγκεκριμένης Ηλεκτρονικής Σφραγίδας (Αρθρ. 40 του Κανονισμού eIDAS) ☐ Διαφύλαξη εγκεκριμένης Ηλεκτρονικής Υπογραφής (Αρθρ. 34 του Κανονισμού eIDAS) ☐ Διαφύλαξη εγκεκριμένης Ηλεκτρονικής Σφραγίδας (Αρθρ. 40 του Κανονισμού eIDAS) ☐ Δημιουργία εγκεκριμένης Ηλεκτρονικής Χρονοσφραγίδας (Αρθρ. 42 του Κανονισμού eIDAS) ☐ Υπηρεσία Συστημένης Παράδοσης (Αρθρ. 44 του Κανονισμού eIDAS) ☐ Πιστοποίηση Γνησιότητας Ιστοτόπων (Αρθρ. 45 του Κανονισμού eIDAS)

ΜΕΡΟΣ Γ – ΟΙΚΟΝΟΜΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ
Πληροφορίες σχετικές με τις οικονομικές πηγές του Παρόχου θα επισυναφθούν. Οι οικονομικές πηγές αποτελούνται από: ☐ Κεφαλαιακή επάρκεια (Ίδια κεφάλαια) ☐ Ασφάλειες ☐ Και τα παραπάνω δυο

Με σχόλια [DZ68]: Προτείνεται να ακολουθηθεί η ορολογία του Κανονισμού, Άρθρο 3 ορισμός 16, ορίζονται συγκεκριμένες «Υπηρεσίες Εμπιστοσύνης»:
1.Δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών υπογραφών (e-Signatures)
2.Δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών σφραγίδων (e-Seals)
3.Δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών χρονοσφραγίδων (Time Stamping)
4.Δημιουργία, εξακρίβωση και επικύρωση πιστοποιητικών για επαλήθευση ταυτότητας ιστοτόπων (Web Site Authentication)
5.Ηλεκτρονικές υπηρεσίες συστημένης παράδοσης (e-Delivery)
6.Ηλεκτρονικές υπηρεσίες διαφύλαξης ηλεκτρονικών υπογραφών, σφραγίδων ή πιστοποιητικών (e-Preservation)

☐ Άλλο

Η εσωκλειόμενες πληροφορίες θα πρέπει να αποδεικνύουν επαρκείς οικονομικούς πόρους για να ανταπεξέλθει η εταιρία στις από νόμο υποχρεώσεις της σύμφωνα και με τις απαιτήσεις του νόμου των Ηλεκτρονικών Υπογραφών.

ΜΕΡΟΣ Δ – ΕΞΑΝΤΛΗΤΙΚΟΣ ΚΑΤΑΛΟΓΟΣ ΤΩΝ ΕΠΙΣΥΝΑΠΤΟΜΕΝΩΝ ΕΓΓΡΑΦΩΝ

- ☐ Έκθεση Αξιολόγησης της Συμμόρφωσης (ΕΑΣ)
- ☐ Αντίγραφο της τυποποιημένης Σύμβασης
- ☐ Πολιτική Υπηρεσίας Εμπιστοσύνης (Trust Service Policy) και Δήλωση Πρακτικής του Παρόχου (Trust Service Practice Statement) για τις υπηρεσίες των οποίων την έγκριση αιτείται, , συνοδευόμενα από ένα ενεργό και έγκυρο URL, όπου είναι δημοσιευμένα τα εν λόγω έγγραφα
- ☐ Δείγματα (Test samples) των πιστοποιητικών ή άλλων στοιχείων που θα εκδοθούν ή θα δημιουργηθούν ως μέρος της υπό έγκριση υπηρεσίας
- ☐ Δικαιολογητικά ανάλογα με την νομική μορφή
- ☐ Πιστοποιητικά εκδοθέντα από τις αρμόδιες Δημόσιες ή Δικαστικές Υπηρεσίες από τα οποία να προκύπτει αν τελεί υπό πτώχευση, πτωχευτικό συμβιβασμό, αναγκαστική διαχείριση ή αν έχουν κατατεθεί σχετικές προς αυτά αιτήσεις καθώς και αν τελεί υπό εκκαθάριση
- ☐ Πιστοποιητικό ασφαλιστικής
- ☐ Πιστοποιητικό φορολογικής ενημερότητας
- ☐ Ισολογισμούς τουλάχιστον των τριών (3) τελευταίων ετών, που έχουν ολοκληρωθεί
- ☐ Αποτίμηση κινδύνου
- ☐ Σχέδιο Ειδοποίησης του τελικού χρήστη
- ☐ Σχέδιο Τερματισμού λειτουργίας

ΜΕΡΟΣ Ε – ΚΟΙΝΟΠΟΙΗΣΗ / ΔΗΜΟΣΙΟΠΟΙΗΣΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η ΕΕΤΤ διατηρεί επικαιροποιημένες πληροφορίες σχετικές με την παροχή Υπηρεσιών Εμπιστοσύνης στη διεύθυνση:
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/EsignProviders.html
Επιθυμείτε να συνδεθεί ο Ιστότοπός σας με αυτόν της ΕΕΤΤ; Παρακαλώ σημειώστε :

- ☐ ΝΑΙ, αν ναι εισάγετε την διεύθυνσή σας εδώ:
- ☐ ΟΧΙ

ΜΕΡΟΣ ΣΤ – ΥΠΟΓΡΑΦΗ

Ο παρακάτω υπογράφων δηλώνω πως πληρούνται όλες οι απαιτήσεις του Νόμου και των Κανονισμών που σχετίζονται με τα εγκεκριμένα πιστοποιητικά και ότι όλες οι παρεχόμενες πληροφορίες είναι ορθές.
Ημερομηνία: Τόπος:
Υπογραφή Νόμιμου Εκπροσώπου

Παράρτημα 5
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 ονόματός του ΠΥΕ και, κατά περίπτωση, του αριθμού εγγραφής, όπως αναφέρεται στα επίσημα αρχεία, της επίσημης ταχυδρομικής διεύθυνσης και της Ηλεκτρονικής Διεύθυνσης Επικοινωνίας.
(Iii) Ταυτοποίηση της σχετικής εγκεκριμένης υπηρεσίας εμπιστοσύνης.

2. Εισαγωγή
Αυτή η παράγραφος προσδιορίζει και εισάγει το σύνολο των προβλέψεων και υποδεικνύει τον ΠΥΕ και τους τύπους υπηρεσιών εμπιστοσύνης που αφορά το σχέδιο τερματισμού.

2.1. Επισκόπηση
Αυτή η παράγραφος παρέχει μια γενική επισκόπηση του σχεδίου τερματισμού και μια σύνοψη του ΠΥΕ/εγκεκριμένης υπηρεσίας εμπιστοσύνης που αφορούν οι διατάξεις τερματισμού. Ανάλογα με την πολυπλοκότητα και το εύρος της υπηρεσίας μπορεί να είναι χρήσιμη μια διαγραμματική αναπαράσταση. Όλοι οι συμμετέχοντες και η υπηρεσία πρέπει να προσδιοριστούν 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 αναγνώριση των εγκεκριμένων υπηρεσιών για τις οποίες ισχύουν οι διατάξεις τερματισμού, ιδίως, όσον αφορά τις αντίστοιχες καταχωρίσεις και τις αντίστοιχες εθνικές υπηρεσίες του Καταλόγου Εμπιστοσύνης και σχετικά με "υπηρεσίεες ψηφιακής ταυτότητας" στοιχεία (δηλ. Δημόσια κλειδιά όταν βασίζονται σε PKI). Εξαρτάται από την πολυπλοκότητα και το εύρος της παροχής υπηρεσίας, το αν θα είναι χρήσιμη μια διαγραμματική απεικόνιση ή ένας πίνακας.

Με σχόλια [DZ69]: Δεν είναι κατανοητή η πρόταση. Χρειάζεται επαναδιατύπωση.

2.4. Διαχείριση σχεδίου τερματισμού
Αυτή η παράγραφος παρέχει το όνομα και τη ταχυδρομική διεύθυνση 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/εγκεκριμένης υπηρεσίας εμπιστοσύνης, στην αναθεώρηση του σχεδίου τερματισμού, στις δοκιμές και στις διαδικασίες ελέγχου, και στην εκτέλεση της. Η παράγραφος περιλαμβάνει επίσης το όνομα, τη διεύθυνση ηλεκτρονικού ταχυδρομείου, τον αριθμό τηλεφώνου και τον αριθμό φαξ του υπευθύνου επικοινωνίας, την θέση του ή τον λειτουργικό του ρόλο.

Με σχόλια [DZ70]: Μπορεί να είναι κάποιος άλλος εκτός από τον ίδιο τον Πάροχο;

2.5. Εφαρμοστέα εθνική νομοθεσία και σχετικές διατάξεις για τον τερματισμό του ΠΥΕ/εγκεκριμένης υπηρεσίας εμπιστοσύνης
Αυτή η παράγραφος παρέχει αναφορές στην ισχύουσα Εθνική Νομοθεσία και προσδιορίζει τις σχετικές
Εθνικές διατάξεις για τον τερματισμό του ΠΥΕ/εγκεκριμένης υπηρεσίας εμπιστοσύνης.

3. Διατάξεις σχετικές με τον τερματισμό

3.1. Προγραμματισμένος τερματισμός

Ο προγραμματισμένος τερματισμός μπορεί να συμβεί στις εξής περιπτώσεις:

- Συγχώνευση με την ενσωμάτωση μιας νομικής οντότητας στη μητρική εταιρεία, των δύο προηγουμένως διακριτών νομικών οντοτήτων (διαφορετικό ~~ΦΠΑ~~ ΑΦΜ και αριθμοί εγγραφής).
- Αλλαγή ονόματος μιας μόνο νομικής οντότητας (ίδιος ~~αριθμός ΦΠΑ~~ΑΦΜ και αριθμός εγγραφής, αλλά άλλο όνομα νομικής οντότητας).
- Πλήρης παροπλισμός στο τέλος του κύκλου ζωής των εξαρτημάτων που βασίζονται σε PKI (π.χ. CAs, μονάδες ~~χρονικής σφράγισης~~χρονοσφραγίδων, QERDS δημιουργών τεκμηρίων) μπορεί να θεωρηθεί ως συγκεκριμένος τερματισμός της Υπηρεσίας Εμπιστοσύνης.
- Σε σχέση με μια υπηρεσία που έχει καταχωρηθεί ως εγκεκριμένη υπηρεσία CA/QC, ο ΠΥΕ ενδέχεται να αποφασίσει να σταματήσει να εκδίδει νέα πιστοποιητικά, αλλά να διατηρεί όλες τις άλλες υπηρεσίες μέχρι την ανάκληση και τη λήξη όλων των προηγουμένως εκδοθέντων εγκεκριμένων πιστοποιητικών.
- Όταν χρησιμοποιείται για την έκδοση διαφόρων τύπων εγκεκριμένων πιστοποιητικών μια εγκεκριμένη υπηρεσία CA/QC, ο ΠΥΕ μπορεί να αποφασίσει:
    - να παύσει την παροχή εγκεκριμένων πιστοποιητικών μόνο ορισμένων τύπων και να συνεχίσει να εκδίδει άλλου τύπου πιστοποιητικά ή εγκεκριμένα πιστοποιητικά ή
    - να παύσει την παροχή όλων των τύπων εγκεκριμένων πιστοποιητικών, αλλά να συνεχίσει να εκδίδει μη εγκεκριμένα πιστοποιητικά.
    - να παύσει την παροχή όλων των τύπων εγκεκριμένων πιστοποιητικών.

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.
- Ταυτοποίηση των δραστηριοτήτων που πρόκειται να παύσουν και αναμενόμενο χρονοδιάγραμμα και σχετικός προγραμματισμός.
- Προσδιορισμός του αναμενόμενου αντίκτυπου στις σχετικές καταχωρήσεις του Καταλόγου Εμπιστοσύνης.
- Επικαιροποίηση της ανάλυσης κινδύνου και επικαιροποιημένα μέτρα μετριασμού του.
- Επικαιροποίηση της εκτίμησης των επιπτώσεων για τα δεδομένα προσωπικού χαρακτήρα και επικαιροποιημένα μέτρα μετριασμού των.
- Ειδοποιήσεις τερματισμού.

Η παράγραφος αυτή περιγράφει τις οντότητες που πρέπει να ενημερωθούν για τον τερματισμό π.χ. ΕΕΤΤ, χρήστες, εμπλεκόμενα μέρη, άλλοι ΠΥΕ που μπορεί να επηρεάζονται, προσωπικό του ΠΥΕ ή/και υπεργολάβους. Για κάθε κοινοποιημένη οντότητα ή λογική ομάδα κοινοποιημένων οντοτήτων, αναφέρονται οι διατάξεις σχετικά με τον τερματισμό, τα μέσα κοινοποίησης και το αναμενόμενο Χρονοδιάγραμμα και ο προγραμματισμός αυτών των κοινοποιήσεων.

~~Συνδεδεμένα~~ Συμπληρωματικά έγγραφα

Η παράγραφος αυτή περιλαμβάνει τις υπηρεσίες των οποίων ο τερματισμός είναι προγραμματισμένος, το λόγο για τον οποίο γίνεται, το αναμενόμενο χρονοδιάγραμμα και το σχετικό προγραμματισμό και τους όρους και προϋποθέσεις που διέπουν την κοινοποίηση του τερματισμού. Περιλαμβάνονται ζητήματα όπως:

Με σχόλια [DZ71]: Να επεξηγηθεί το ακρωνύμιο

Με σχόλια [DZ72]: Άγνωστο ακρωνύμιο.

Με σχόλια [DZ73]: Δεν είναι κατανοητή η διατύπωση όλης της πρότασης.

Με σχόλια [DZ74]: Να προστεθεί επεξήγηση για όσους δεν γνωρίζουν το ETSI TS 119 612 πρότυπο των Trust Lists

Με σχόλια [DZ75]: Οι σχετικές καταχωρήσεις της TSL δεν μπορούν να χαρακτηριστούν ως «αντίκτυπος» αλλά ως μια φυσιολογική συνέπεια της πράξης τερματισμού. Προτείνεται να γίνει «Προσδιορισμός των προτεινόμενων αλλαγών στις σχετικές καταχωρήσεις του Καταλόγου Εμπιστοσύνης», αν και αυτό είναι αρμοδιότητα της Εποπτεύουσας Αρχής.

- 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.
- Όσον αφορά τα εγκεκριμένα πιστοποιητικά, οι όροι για τη συνέχιση της χρήσης ή της ανάκλησής των πιστοποιητικά που δεν έχουν λήξει.
- Προβλεπόμενες αποζημιώσεις στους συνδρομητές, κατά περίπτωση.

Διαδικασίες εκτέλεσης των ενεργειών τερματισμού

- Ταυτοποίηση του προσωπικού (του ΠΥΕ ή/και υπεργολάβων), της απαιτούμενης εμπειρίας τους και των συνθήκων της σχετικής κατάρτισης τους.
- Μεταφορά των καταγεγραμμένων, ελεγκτικών και αρχειακών εγγραφών στον (στους) συμβεβλημένο -(ους) μεσάζοντα (-ες) και την κατάλληλη ταυτοποίηση του(ς).

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 αιτιών τερματισμού και τις απαιτούμενες σημαντικές μειώσεις των καθυστερήσεων εντός των οποίων πρέπει να αναληφθούν οι σχετικές δράσεις αυτές. Στην παράγραφο αυτή θα πρέπει να καθοριστούν 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 θεμάτων 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.
- Την ταυτότητα ή / και τα προσόντα του προσωπικού που εκτελεί τον έλεγχο τερματισμού του σχεδίου.
- 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.
- Τον κατάλογο των θεμάτων που καλύπτονται από την αξιολόγηση ή/και τη μεθοδολογία αξιολόγησης που χρησιμοποιήθηκε κατά την αξιολόγηση.
- Τη Συχνότητα ελέγχου συμμόρφωσης ή άλλης αξιολόγησης.

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

3. Ερωτήσεις ΔΔ

1. Αναπτύξτε τα σχόλιά σας στις ανωτέρω προτεινόμενες διατάξεις του Κανονισμού Παροχής Υπηρεσιών Εμπιστοσύνης
2. Έχετε να προσθέσετε/προτείνετε κάτι άλλο που θεωρείτε σημαντικό και δεν έχει αναφερθεί παραπάνω; Αναλύστε και αιτιολογήστε τις προτάσεις σας.

Σελίδα 8: [1] Με σχόλια [DZ26]	Dimitris Zacharopoulos	11/10/2017 12:24:00 μμ

Το συγκεκριμένο φαίνεται να είναι πρόβλημα επιπέδου 2. Δεν επηρεάζει τον συνδρομητή ο οποίος απλά θα πρέπει να δοκιμάσει αργότερα. Δεν υπάρχει κάποια άμεση «ζημία» στον συνδρομητή από τη μη διαθεσιμότητα της υπηρεσίας.

Σελίδα 8: [2] Με σχόλια [DZ28]	Dimitris Zacharopoulos	11/10/2017 12:26:00 μμ

Φαίνεται να είναι πρόβλημα επιπέδου 2 λόγω του ότι ο χρήστης θα είναι δυσαρεστημένος με τη μη διαθεσιμότητα. Δεν επηρεάζει άμεσα τον συνδρομητή ο οποίος απλά θα πρέπει να δοκιμάσει αργότερα. Δεν υπάρχει κάποια άμεση «ζημία» στον συνδρομητή από τη μη διαθεσιμότητα της υπηρεσίας εκτός αν υπάρχει παρατεταμένη διακοπή. Προτείνεται να γίνει «Υποβαθμισμένη ή μη διαθέσιμη υπηρεσία εμπιστοσύνης για σημαντικό χρονικό διάστημα» κι αν θέλει η ΕΕΤΤ, ας προσδιορίσει ποιο θα ήταν αυτό το «σημαντικό» διάστημα.

Σελίδα 8: [3] Με σχόλια [DZ29]	Dimitris Zacharopoulos	11/10/2017 12:27:00 μμ

Φαίνεται να είναι πρόβλημα επιπέδου 2 και σε κάθε περίπτωση υπάρχει δυνατότητα ανάκτησης από αντίγραφα ασφαλείας. Δεν επηρεάζεται ο συνδρομητής ο οποίος έχει ήδη ψηφιακό πιστοποιητικό με τα σωστά στοιχεία. Αν τα στοιχεία του Πιστοποιητικού είναι εσφαλμένα, τότε εμπίπτει στην περίπτωση 5.2.3. Προτείνεται να αφαιρεθεί.