ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

ΤΕΥΧΟΣ ΔΗΜΟΣΙΑΣ ΔΙΑΒΟΥΛΕΥΣΗΣ

Θέμα: Ρύθμιση ειδικότερων ζητημάτων της παροχής εγκεκριμένων υπηρεσιών εμπιστοσύνης και της ανάκλησης εγκεκριμένων πιστοποιητικών

Μαρούσι, Νοέμβριος 2021

Το παρόν Τεύχος Δημόσιας Διαβούλευσης έχει ετοιμαστεί από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και αφορά στη ρύθμιση ειδικότερων ζητημάτων της παροχής εγκεκριμένων υπηρεσιών εμπιστοσύνης και ανάκλησης εγκεκριμένων πιστοποιητικών.

Η ΕΕΤΤ προσκαλεί τους ενδιαφερόμενους φορείς να υποβάλουν τα σχόλια και τις απόψεις τους σχετικά με την πρότασή της, όπως διαμορφώνεται στο παρόν Τεύχος Δημόσιας Διαβούλευσης, προκειμένου να υποβληθεί εν συνεχεία η εισήγηση της ΕΕΤΤ για την έκδοση Υ.Α. σύμφωνα με τα προβλεπόμενα στο άρθρο 107 παρ. 31 και 34 του ν. 4727/2020 (ΦΕΚ 184 Α).

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

Οι απαντήσεις πρέπει να υποβληθούν επωνύμως, στην Ελληνική γλώσσα, σε έντυπη ή/και σε ηλεκτρονική μορφή στην ηλεκτρονική διεύθυνση eidas@eett.gr όχι αργότερα από την **17η Δεκεμβρίου 2021** και ώρα 16:00. 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 έχει δικαίωμα να δημοσιεύσει τα ονόματα των συμμετεχόντων στη ΔΔ. Οι συμμετέχοντες στις δημόσιες διαβουλεύσεις της ΕΕΤΤ είναι ενήμεροι και συναινούν ότι τυχόν προσωπικά στοιχεία που αναφέρονται πάνω στην απάντησή τους ενδέχεται να δημοσιευθούν μαζί με αυτήν. Σχετικά με τη Δήλωση περί απορρήτου και προστασίας δεδομένων προσωπικού χαρακτήρα της ΕΕΤΤ δείτε εδώ:

https://www.eett.gr/opencms/opencms/EETT/privacy.html.

Οι απαντήσεις πρέπει να υποβάλλονται ηλεκτρονικά στην ακόλουθη διεύθυνση ηλεκτρονικού ταχυδρομείου:

E-mail : eidas@eett.gr

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

ΜΕΡΟΣ Α

ΠΡΟΤΕΙΝΟΜΕΝΟ ΠΕΡΙΕΧΟΜΕΝΟ

Υπουργικής Απόφασης άρθρου 107 παρ. 31 του ν.4727/2020

Μέρος Α: Γενικές Διατάξεις

Άρθρο 1

Σκοπός και πεδίο εφαρμογής

Σκοπός της παρούσας είναι η ρύθμιση ειδικότερων ζητημάτων των υπηρεσιών εμπιστοσύνης.

Άρθρο 2

Ορισμοί και Ακρωνύμια

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

Κανονισμός eIDAS: Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ (OJ L257).

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

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

3. Ακρωνύμια

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

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

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

CP : Certificate Policy

CPS : Certificate Practice Statement

CRL : Λίστα Ανακληθέντων Πιστοποιητικών (Certificate Revocation List)

ENISA : Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

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

Root CA : Αρχή Πιστοποίησης Ρίζας

Sub CA : Υποκείμενη Αρχή Πιστοποίησης

Μέρος Β': Αντιστοίχιση υποχρεώσεων με διατάξεις του Κανονισμού eIDAS (όπου απαιτείται)

Άρθρο 3

Απαιτήσεις ασφάλειας (Άρθρα 19 και 24, παρ. 2)

Η ΕΕΤΤ, ως εποπτικός φορέας των εγκεκριμένων ΠΥΕ και των υπηρεσιών που αυτοί παρέχουν, κατά την άσκηση των καθηκόντων της λαμβάνει υπόψη τις συστάσεις που δημοσιεύει ο ENISA για την υλοποίηση των απαιτήσεων που προβλέπονται στα άρθρα 19 και 24, παρ. 2 του Κανονισμού eIDAS. Οι ΠΥΕ οφείλουν να ακολουθούν τις συστάσεις που περιλαμβάνονται στα σχετικά έγγραφα.

Άρθρο 4

Αριθμός μητρώου εγκεκριμένου ΠΥΕ (Παραρτήματα I, III και IV)

1. Ο αριθμός μητρώου του εγκεκριμένου ΠΥΕ που περιλαμβάνεται στο πεδίο Εκδότης (Issuer) στα εγκεκριμένα πιστοποιητικά που εκδίδει, όπως ορίζεται στα Παραρτήματα I, III και IV του Κανονισμού eIDAS, ακολουθεί τα οριζόμενα στο πρότυπο ETSI EN 319 412-1, στην εκάστοτε ισχύουσα έκδοσή του. Ο κωδικός χώρας στην περίπτωση των προθεμάτων "TIN" και "VAT" μπορεί να είναι "EL" ή "GR". Ο κωδικός χώρας σε όλες τις άλλες περιπτώσεις είναι "EL". Η υποχρέωση ισχύει για τα πιστοποιητικά που εκδίδονται μετά τη θέση σε ισχύ της παρούσας Απόφασης. Ειδικά για τις Αρχές Πιστοποίησης που είναι ήδη εγκεκριμένες κατά την έναρξη ισχύος της παρούσας, η συμπερίληψη του αριθμού μητρώου του τελικού πιστοποιητικού μπορεί να γίνει και σε άλλο πεδίο από το πεδίο Εκδότης.
2. Κατόπιν αιτιολογημένου αιτήματος του εγκεκριμένου ΠΥΕ και με τη σύμφωνη γνώμη της ΕΕΤΤ, μπορεί να χρησιμοποιηθεί για το πεδίο αυτό ο αριθμός καταχώρισης του εγκεκριμένου ΠΥΕ στο αρχείο των παρόχων υπηρεσιών εμπιστοσύνης που τηρεί η ΕΕΤΤ. Στην περίπτωση αυτή, οι 2 χαρακτήρες που χρησιμοποιούνται για τον καθορισμό του συγκεκριμένου εθνικού σχήματος είναι "RT". Κατά συνέπεια, η δομή του αριθμού μητρώου στο πεδίο Issuer του τελικού εγκεκριμένου πιστοποιητικού, όπως δηλώνεται μέσω του χαρακτηριστικού *organizationIdentifier* (OID 2.5.4.97), ορίζεται ως: <RT:EL–αριθμός καταχώρισης στο αρχείο της ΕΕΤΤ>.
3. Το αναγνωριστικό "RT:EL" καταχωρίζεται ως αναγνωριστικό σε επίπεδο εποπτικού φορέα (ΕΕΤΤ), σύμφωνα με τα αναφερόμενα στην παρ. 5.4.2 του υποχρεωτικού από την Εκτελεστική Απόφαση της ΕΕ 2015/1505, όπως εκάστοτε ισχύει, προτύπου ETSI TS 119 612.

Άρθρο 5

Αριθμός μητρώου του δημιουργού εγκεκριμένης ηλεκτρονικής σφραγίδας (Παράρτημα ΙΙ)

Ο αριθμός μητρώου του δημιουργού μιας εγκεκριμένης ηλεκτρονικής σφραγίδας, που περιλαμβάνεται στο πεδίο Subject του εγκεκριμένου πιστοποιητικού, όπως ορίζεται στο Παράρτημα III του Κανονισμού eIDAS, ακολουθεί τα οριζόμενα στο πρότυπο ETSI EN 319 412-1, στην εκάστοτε ισχύουσα έκδοσή του. Ο κωδικός χώρας στην περίπτωση του προθέματος "VAT" μπορεί να είναι "EL" ή "GR". Ο κωδικός χώρας σε όλες τις άλλες περιπτώσεις είναι "EL".

Commented [A1]: Ο ENISA, ως μονάδα της ΕΕ, έχει αποκλειστικά συμβουλευτικό χαρακτήρα και όλα τα κείμενα-μελέτες έχουν αυτή τη λογική. Κανένα έγγραφο «προτάσεων» του ENISA δεν έχει λάβει το βαθμό ανάλυσης που αρμόζει σε «Κανονιστικό» πλαίσιο προκειμένου να απαιτηθεί να ακολουθείται-εφαρμόζεται στο σύνολό του. Ο ENISA έχει δημοσιεύσει μεγάλο αριθμό εγγράφων σχετικά με τον Κανονισμό eIDAS.

Εφόσον η ΕΕΤΤ κρίνει ότι **κάποια σημεία συγκεκριμένων μελετών του ENISA** έχουν την ωριμότητα, αξιοπιστία, αποδοχή της πλειοψηφίας της συγκεκριμένης βιομηχανίας και των Ευρωπαϊκών Εποπτικών Αρχών, προτείνουμε να υπάρξει **συγκεκριμένη μελλοντική απόφαση της ΕΕΤΤ ή του ΥΨηΔ** που να ορίζει την υποχρέωση εφαρμογής των συγκεκριμένων αυτών σημείων προς τους ΠΥΕ με συγκεκριμένη **μελλοντική** ημερομηνία έναρξης εφαρμογής (πχ σε 12 μήνες από τη δημοσίευση).

Commented [A2]: Σύμφωνα με τα Διεθνή Πρότυπα, καθώς και το ETSI EN 319 412-1, η εξαίρεση για το "EL" ισχύει ΜΟΝΟ για τα προθέματα "TIN" και "VAT". Σε όλες τις άλλες περιπτώσεις οφείλει να είναι **"GR"** σύμφωνα με την επίσημη alpha-2 καταχώρηση της χώρας μας στο ISO 3166-1. Για παράδειγμα, χρήση της τιμής "EL" στο πεδίο countryName αποτελεί παραβίαση των προτύπων ETSI EN 319 412-1, CA/B Forum Baseline Requirements (επηρεάζει τα εγκεκριμένα πιστοποιητικά ιστοχώρων).
Συστήνεται να αλλάξει η τιμή "EL" σε "GR".

Αξίζει να σημειωθεί ότι το πρότυπο ETSI EN 319 412-1 εφαρμόζεται μόνο για όσους παρόχους **επιθυμούν** να δώσουν σήμανση "semantics identifier" (Natural ή Legal) μέσω των πεδίων organizationIdentifier και serialNumber.

Επιπλέον, να διευκρινιστεί ποιες είναι όλες οι «άλλες περιπτώσεις» καθώς η συγκεκριμένη απαίτηση είναι αόριστη με αποτέλεσμα να είναι αδύνατος ο έλεγχος συμμόρφωσης.

Commented [A3]: Απαιτείται διάστημα προσαρμογής για οποιαδήποτε απόφαση χρειάζεται τεχνικές αλλαγές σε παραγωγικά συστήματα ΠΥΕ. Ένα ελάχιστο διάστημα έξι (6) μηνών δεν είναι απαγορευτικό για αυτού του είδους τις αλλαγές καθώς εμπλέκονται πολιτικές αλλαγών (change management policies), εγκρίσεις, περίοδος δοκιμών ακόμα και για τις πιο απλές αλλαγές.

Commented [A4]: Στην περίπτωση αυτή, εφόσον κάποιος ΠΥΕ αποφασίσει να αξιοποιήσει τη συγκεκριμένη επιλογή, σύμφωνα με το πρότυπο ETSI EN 319 412-1, ισχύει υποχρεωτικά και η τελευταία παράγραφος της ενότητας 5.1.4 η οποία αναφέρει:

"When a locally defined identity type reference is provided (two characters followed by ":"), the `nameRegistrationAuthorities` *element of* `SemanticsInformation` *(IETF RFC 3739 [1]) shall be present and shall contain at least a* `uniformResourceIdentifier` *or* `generalName`*. The two letter identity type reference following the ":" character shall be unique within the context of the specified* `uniformResourceIdentifier`*."*

Για λόγους συνέπειας-πληρότητας, προτείνεται να προστεθεί και η συγκεκριμένη απαίτηση ή παραπομπή στο ETSI EN 319 412-1 ενότητα 5.1.4.

Commented [A5]: Παράρτημα III αντί για II. Για ακόμα μεγαλύτερη σαφήνεια, προτείνεται να αναφερθεί το «Παράρτημα III σημείο γ)»

Commented [A6]: Ισχύουν οι ίδιες παρατηρήσεις-επισημάνσεις για το "EL" ή "GR" που αφορούν και στον αρ. μητρώου ΠΥΕ (Άρθρο 4).

Άρθρο 6

Χρήση ψευδωνύμων (Παραρτήματα I και IV)

Το όνομα του φυσικού προσώπου, στο οποίο έχει εκδοθεί το εγκεκριμένο πιστοποιητικό, δηλώνεται κατάλληλα στα στοιχεία *surname* (OID 2.5.4.4) και *givenName* (OID 2.5.4.42) στο πεδίο *Subject*. Αν χρησιμοποιείται ψευδώνυμο τότε αυτό δηλώνεται στο στοιχείο *pseudonym* (OID 2.5.4.65) συνοδευόμενο από κατάλληλη αναφορά στο στοιχείο *commonName* (OID 2.5.4.3), όπου τουλάχιστον η λέξη "PSEUDONYM" πρέπει να περιλαμβάνεται.

Commented [A7]: Δεν έχουν οριστεί διεθνώς ικανοποιητικά κριτήρια επαλήθευσης στοιχείων για ψευδώνυμα, με συνέπεια οι πλειονότητα των ΠΥΕ να μη χρησιμοποιούν αυτά τα πεδία. Εφόσον κρίνεται σκόπιμη η υποστήριξη αυτής της δυνατότητας, προτείνεται στο Άρθρο 6 να δοθούν παραδείγματα από αποδεκτές πρακτικές από την ΕΕΤΤ για την εξακρίβωση ψευδωνύμων από τους ΠΥΕ, ώστε οι επαληθευμένες αυτές πληροφορίες να μπορούν να εισαχθούν σε εγκεκριμένο πιστοποιητικό.

Ελλείψει ικανοποιητικών/αποδεκτών πρακτικών επαλήθευσης, θα ήταν πιο ασφαλής η καθολική απαγόρευση χρήσης ψευδώνυμων.

Άρθρο 7

Περιεχόμενο τελικών πιστοποιητικών

1. Το περιεχόμενο των τελικών πιστοποιητικών που εκδίδονται σε φυσικά πρόσωπα ακολουθεί τα οριζόμενα στο πρότυπο ETSI EN 319 412-2, στην εκάστοτε ισχύουσα έκδοσή του, εκτός από τα σημεία που ορίζεται διαφορετικά στην παρούσα.
2. Το περιεχόμενο των τελικών πιστοποιητικών που εκδίδονται σε νομικά πρόσωπα ακολουθεί τα οριζόμενα στο πρότυπο ETSI EN 319 412-3, στην εκάστοτε ισχύουσα έκδοσή του, εκτός από τα σημεία που ορίζεται διαφορετικά στην παρούσα.

Άρθρο 8

Απαιτήσεις σχετικά με την ταυτοποίηση (άρθρο 24, παρ. 1)

1. Εφόσον η έκδοση εγκεκριμένου πιστοποιητικού βασίζεται σε ταυτοποίηση η οποία γίνεται με φυσική παρουσία του φυσικού προσώπου ή του εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου (άρθρο 24, παρ. 1, στοιχείο α) του Κανονισμού eIDAS), η ταυτοποίηση πρέπει να έχει διενεργηθεί εντός ενός (1) έτους από την έκδοση.
2. Εφόσον η έκδοση εγκεκριμένου πιστοποιητικού βασίζεται σε ταυτοποίηση η οποία γίνεται με κάποια από τις άλλες μεθόδους ταυτοποίησης του άρθρου 24, παρ. 1 (στοιχεία β, γ και δ) του Κανονισμού eIDAS, η ταυτοποίηση πρέπει να έχει διενεργηθεί εντός ενός (1) μηνός από την έκδοση.

Commented [A8]: Σύμφωνα με τον Κανονισμό η μέθοδος δ) έχει ελεγχθεί ότι είναι ισοδύναμη με το α) συνεπώς θεωρούμε ότι ταιριάζει να μεταφερθεί στην πρώτη παράγραφο μαζί με το α) και να έχει και την ίδια ισχύ 1 έτος.

3. Εφόσον κατά την έκδοση εγκεκριμένου πιστοποιητικού, χρησιμοποιείται για την ταυτοποίηση εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής (άρθρο 24, παρ. 1, στοιχείο γ) του Κανονισμού eIDAS), ισχύουν οι εξής προϋποθέσεις για το εγκεκριμένο πιστοποιητικό:
   α) Να είναι σε ισχύ. Ο ΠΥΕ οφείλει να εξακριβώνει ότι ικανοποιούνται όλες οι απαιτήσεις της παρ. 1 του άρθρου 32 του Κανονισμού eIDAS.
   β) Να έχει εκδοθεί με μία εκ των μεθόδων των στοιχείων α), β) και δ) του άρθρου 24, παρ. 1 του Κανονισμού eIDAS. Ο εγκεκριμένος ΠΥΕ υποχρεούται να ελέγχει ότι τηρείται αυτή η απαίτηση και να τηρεί στο αρχείο του όλα τα απαραίτητα στοιχεία που αποδεικνύουν με ποια μέθοδο ταυτοποίησης εκδόθηκε το συγκεκριμένο πιστοποιητικό.
4. Κάθε εγκεκριμένος ΠΥΕ υποχρεούται να παρέχει την πληροφορία σχετικά με τον τρόπο ταυτοποίησης που χρησιμοποίησε για την έκδοση εγκεκριμένου πιστοποιητικού, που είναι σε ισχύ, σε άλλον εγκεκριμένο ΠΥΕ, κατόπιν αιτιολογημένου αιτήματος του τελευταίου, το αργότερο εντός τριών (3) ημερών από την υποβολή του.

Commented [A9]: Η συγκεκριμένη απαίτηση θα δημιουργήσει στρεβλώσεις στην αγορά καθώς:

α) παρόμοια απαίτηση δεν ισχύει σε άλλα Κράτη Μέλη με αποτέλεσμα να μη μπορεί να ζητηθούν αυτά τα στοιχεία από ΠΥΕ που δραστηριοποιούνται εκτός Ελλάδας. Οι ΠΥΕ του εξωτερικού θα μπορούν να λαμβάνουν στοιχεία από τους ΠΥΕ της Ελλάδας ενώ δεν θα ισχύει το αντίστροφο

β) μπορεί να αποτελέσει πεδίο πιθανής κατάχρησης όπου ένας ΠΥΕ μπορεί να καταθέτει διαρκώς αιτήματα σε άλλους ΠΥΕ προκαλώντας αυξημένο φόρτο εργασίας.

Επίσης η προθεσμία των 3 ημερών είναι πολύ περιοριστική και είναι πρακτικά αδύνατο να ανταποκριθεί ένας ΠΥΕ σε αιτήματα άλλων ΠΥΕ, ιδιαίτερα σε περιόδους αργιών/διακοπών.

Προτείνεται να καταργηθεί η παρ.4 ή να αναπτυχθεί από την ΕΕΤΤ ένα Εθνικό Πληροφοριακό Σύστημα ώστε η συγκεκριμένη πληροφορία να καταγράφεται κεντρικά και να είναι διαθέσιμη σε όποιον ΠΥΕ το αιτείται.

Άρθρο 9

Υποχρέωση καταγραφής και διατήρησης πληροφοριών (Άρθρο 24 παρ. 2 περ. η΄ Κανονισμού eIDAS)

Οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης κατά την έκδοση εγκεκριμένου πιστοποιητικού, καταχωρίζουν στο αρχείο που τηρούν και διατηρούν προσβάσιμα, μεταξύ άλλων, τα ακόλουθα:

α) Όταν πρόκειται για εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής:

i. Την αίτηση έκδοσης εγκεκριμένου πιστοποιητικού πλήρως συμπληρωμένη με όλα τα απαραίτητα στοιχεία. Η αίτηση πρέπει να φέρει την ιδιόχειρη ή εγκεκριμένη ηλεκτρονική υπογραφή του αιτούντα και να έχει υποβληθεί σε διάστημα όχι μεγαλύτερο των τριών (3) μηνών πριν από την ημερομηνία έκδοσης του πιστοποιητικού. Σε περίπτωση που υπογράφεται με εγκεκριμένη ηλεκτρονική υπογραφή συστήνεται χρήση εγκεκριμένης χρονοσφραγίδας.

ii. Τους όρους χρήσης της υπηρεσίας, όπως ίσχυαν κατά το χρόνο υποβολής της αίτησης, υπογεγραμμένους από τον αιτούντα με ιδιόχειρη ή εγκεκριμένη ηλεκτρονική υπογραφή, οπότε και συστήνεται η χρήση εγκεκριμένης χρονοσφραγίδας, άλλως με αποδοχή των όρων από τον αιτούντα μέσω κατάλληλης επιλογής στην ιστοσελίδα του παρόχου. Στην τελευταία περίπτωση ο ΠΥΕ οφείλει να εξακριβώνει κατάλληλα την ταυτότητα του «υπογράφοντα» και να διασφαλίζει ότι η ημερομηνία και ώρα της αποδοχής καταγράφεται στο αρχείο.

β) Όταν πρόκειται για εγκεκριμένο πιστοποιητικό ηλεκτρονικής σφραγίδας:

i. Την αίτηση έκδοσης εγκεκριμένου πιστοποιητικού πλήρως συμπληρωμένη- με όλα τα απαραίτητα στοιχεία. Η αίτηση πρέπει να φέρει την ιδιόχειρη ή εγκεκριμένη ηλεκτρονική υπογραφή του νόμιμου εκπροσώπου ή του ειδικά εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου ή την εγκεκριμένη ηλεκτρονική σφραγίδα του νομικού προσώπου και να έχει υποβληθεί σε διάστημα όχι μεγαλύτερο των τριών (3) μηνών πριν από την ημερομηνία έκδοσης του πιστοποιητικού. Σε περίπτωση που υπογράφεται με εγκεκριμένη ηλεκτρονική υπογραφή ή σφραγίζεται με εγκεκριμένη ηλεκτρονική σφραγίδα, συστήνεται η χρήση εγκεκριμένης χρονοσφραγίδας.

ii. Τους όρους χρήσης της υπηρεσίας, όπως ίσχυαν κατά το χρόνο υποβολής της αίτησης, υπογεγραμμένους από τον εξουσιοδοτημένο εκπρόσωπο του νομικού προσώπου με ιδιόχειρη ή εγκεκριμένη ηλεκτρονική υπογραφή ή σφραγισμένους με την εγκεκριμένη ηλεκτρονική σφραγίδα του νομικού προσώπου. Στη δεύτερη και τρίτη περίπτωση συστήνεται η χρήση εγκεκριμένης χρονοσφραγίδας.

Άρθρο 10

Αποθήκευση εγκεκριμένου πιστοποιητικού σε ΕΔΔΥ

Κατά την έκδοση εγκεκριμένου πιστοποιητικού εγκεκριμένης ηλεκτρονικής υπογραφής ή εγκεκριμένης ηλεκτρονικής σφραγίδας, ο εγκεκριμένος ΠΥΕ οφείλει, εκτός των άλλων, να διασφαλίζει ότι:

α) Ο κάτοχος του πιστοποιητικού μπορεί, με υψηλό βαθμό εμπιστοσύνης και υπό τον αποκλειστικό του έλεγχο, να δημιουργεί τα δεδομένα ηλεκτρονικής υπογραφής ή σφραγίδας (άρθρο 26, παρ. γ του Κανονισμού eIDAS), όταν δεν χρησιμοποιείται διάταξη απομακρυσμένης ηλεκτρονικής υπογραφής ή σφραγίδας.

β) Η ΕΔΔΥ ικανοποιεί τις απαιτήσεις του Παραρτήματος ΙΙ του Κανονισμού eIDAS και περιλαμβάνεται στον κατάλογο που δημοσιεύει η Ευρωπαϊκή Επιτροπή, σύμφωνα με το άρθρο 31, παρ. 2 του Κανονισμού eIDAS.

Commented [A10]: Είναι οξύμωρο να απαιτείται εγκεκριμένη ηλ. υπογραφή σε αίτηση εγκεκριμένης ηλ. υπογραφής και ισχύει μόνο στην περίπτωση εξακρίβωσης στοιχείων με την περίπτωση 1γ του Άρθρου 24 του Κανονισμού.

Κάθε Πάροχος ορίζει, στις διαδικασίες του, ποια στοιχεία ζητούνται από τον αιτούντα. Η **αίτηση** μπορεί να υποβάλλεται με ηλεκτρονικά μέσα και να καταγράφονται τα στοιχεία αυτής για το Αρχείο, καλύπτοντας πλήρως τις απαιτήσεις του Κανονισμού. Συνεπώς, ο περιορισμός που θέτει η ΕΕΤΤ (είτε ιδιόχειρη είτε εγκεκριμένη ηλ. Υπογραφή σε κάθε αίτηση) δε συνάδει με τις τρέχουσες διεθνείς πρακτικές και αποτελεί παρέμβαση που ξεφεύγει από το πνεύμα και το γράμμα του Κανονισμού, ο οποίος είναι τεχνολογικά ουδέτερος ενώ ταυτόχρονα δεν θέτει τόσο αυστηρές υποχρεώσεις για τον τρόπο που ένας Πάροχος θα **δέχεται αιτήσεις** συγκεκριμένων προϊόντων/υπηρεσιών. Η εξακρίβωση ταυτότητας είναι υποχρεωτική σε κάθε περίπτωση και γίνεται σύμφωνα με τα όσα αναφέρονται στην παρ. 1 του Άρθρου 24.

Στην επόμενη υπο-ενότητα "ii", σωστά δίνεται επιλογή της αίτησης με ηλεκτρονικά μέσα όπως μέσω ιστοσελίδας. Προτείνεται να επιτραπεί και στην υπο-ενότητα "i".

Commented [A11]: Παρομοίως, δεν είναι κατανοητό γιατί απορρίπτονται διεθνείς και ασφαλείς πρακτικές **αιτήσεων υπηρεσιών** με ηλεκτρονικά μέσα εκτός των όσων αναφέρονται στην συγκεκριμένη υπο-ενότητα. Η **αίτηση** μπορεί να υποβάλλεται με ηλεκτρονικά μέσα και να καταγράφονται τα στοιχεία αυτής για το Αρχείο, καλύπτοντας πλήρως τις απαιτήσεις του Κανονισμού

Commented [A12]: Στο Άρθρο 26 παρ. γ. δεν αναφέρει ότι τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής πρέπει να τα **δημιουργεί** ο κάτοχος. Αναφέρεται στη **χρήση** υπό τον αποκλειστικό του έλεγχο.

Με βάση τα ανωτέρω, προτείνεται να τροποποιηθεί η συγκεκριμένη απαίτηση ως εξής:
«Ο κάτοχος του πιστοποιητικού μπορεί, με υψηλό βαθμό εμπιστοσύνης και υπό τον αποκλειστικό του έλεγχο, **να δημιουργεί προηγμένες ηλεκτρονικές υπογραφές χρησιμοποιώντας** τα δεδομένα ηλεκτρονικής υπογραφής ή σφραγίδας (άρθρο 26, παρ. γ του Κανονισμού eIDAS), όταν δεν χρησιμοποιείται διάταξη απομακρυσμένης ηλεκτρονικής υπογραφής ή σφραγίδας»

Αν η ΕΕΤΤ επιθυμεί να διασαφηνίσει τις συνθήκες δημιουργίας των δεδομένων δημιουργίας ηλ. Υπογραφής/σφραγίδας, τότε προκειμένου να διασφαλιστεί ότι τα δεδομένα δημιουργίας ηλ. Υπογραφής δημιουργούνται πράγματι εντός Εγκεκριμένων Διατάξεων Δημιουργίας Υπογραφής (ΕΔΔΥ), και σύμφωνα με διεθνείς αποδεκτές πρακτικές, η δημιουργία των δεδομένων δημιουργίας υπογραφής είναι ασφαλές αν γίνεται υπό τον έλεγχο του ΠΥΕ. Στη συνέχεια, η ΕΔΔΥ παραδίδεται στον κάτοχο προκειμένου «να χρησιμοποιεί υπό τον αποκλειστικό του έλεγχο» τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής σύμφωνα με τα οριζόμενα στο Άρθρο 26 παρ. γ.

Το κλειδί μπορεί να δημιουργείται απομακρυσμένα από τον συνδρομητή χωρίς τη μεσολάβηση του ΠΥΕ μόνο αν η ΕΔΔΥ υποστηρίζει από τον κατασκευαστή της **απομακρυσμένο κρυπτογραφικό έλεγχο** στο δημιουργηθέν κλειδί (remote key attestation).

Κατά τη γνώμη μας, ισχύουσες πρακτικές ΠΥΕ όπου μέσω λογισμικού μπορεί να πραγματοποιείται η δημιουργία κλειδιών «εντός συγκεκριμένων ΕΔΔΥ» οι οποίες όμως μπορεί να «προσομοιωθούν» με εικονικές τοπικές συσκευές ώστε το κλειδί να δημιουργηθεί σε λογισμικό αντί για ΕΔΔΥ, με αποτέλεσμα να μην ικανοποιούνται οι προϋποθέσεις του Κανονισμού eIDAS για πιστοποιητικά εγκεκριμένων υπογραφών/σφραγίδων, πρέπει να απαγορευθούν ρητά.

Άρθρο 11

Έναρξη ισχύος εγκεκριμένου πιστοποιητικού και παράδοση στον κάτοχό του

1. Τα εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών και σφραγίδων πρέπει να βρίσκονται στην κατοχή των νόμιμων κατόχων τους από την έναρξη έως τη λήξη της ισχύος τους. Η έκδοση των εγκεκριμένων πιστοποιητικών πρέπει να γίνεται είτε τη στιγμή της παράδοσης της ΕΔΔΥ στο συνδρομητή, οπότε και εγκαθίσταται το εκδοθέν πιστοποιητικό, είτε, στην περίπτωση που η ΕΔΔΥ βρίσκεται ήδη στην κατοχή του συνδρομητή και χρησιμοποιείται αυτοματοποιημένη υπηρεσία απομακρυσμένης εγκατάστασης πιστοποιητικών, που παρέχει ο εγκεκριμένος ΠΥΕ, τη στιγμή που, κατόπιν κατάλληλων ενεργειών του συνδρομητή, δημιουργείται στην ΕΔΔΥ το ζεύγος κλειδιών και εγκαθίσταται το εγκεκριμένο πιστοποιητικό. Στην περίπτωση που η διαχείριση των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας γίνεται από τον εγκεκριμένο ΠΥΕ για λογαριασμό του συνδρομητή, η έκδοση του εγκεκριμένου πιστοποιητικού γίνεται τη στιγμή της αρχικής σύνδεσης και ενεργοποίησης της υπηρεσίας από το συνδρομητή.
2. Η ημερομηνία και ώρα έναρξης της ισχύος ενός εγκεκριμένου πιστοποιητικού, η οποία περιλαμβάνεται σε αυτό σύμφωνα με τα Παραρτήματα Ι και ΙΙΙ του Κανονισμού eIDAS, είναι η ημερομηνία και ώρα που λαμβάνει χώρα το γεγονός που αναφέρεται στην παρ. 1 του παρόντος άρθρου.
3. Κάθε εγκεκριμένος ΠΥΕ οφείλει να καταγράφει στο αρχείο που τηρεί την ημερομηνία και ώρα που έλαβε χώρα το γεγονός που αναφέρεται στην παρ. 1 του παρόντος άρθρου.
4. Σε κάθε περίπτωση, υπογραφές ή σφραγίδες με χρόνο υπογραφής, όπως ορίζεται στο άρθρο 12, παρ. 1 κατωτέρω, που προηγείται της ημερομηνίας και ώρας κατά την οποία το εγκεκριμένο πιστοποιητικό παραδόθηκε στον κάτοχό του, όπως ορίζεται στην παρ. 1 του παρόντος άρθρου, θεωρούνται άκυρες.
5. Στην περίπτωση που παρέχεται αυτοματοποιημένη υπηρεσία απομακρυσμένης εγκατάστασης πιστοποιητικών σε ΕΔΔΥ από εγκεκριμένο ΠΥΕ, ισχύουν τα ακόλουθα:
   α) Δεν επιτρέπεται η μεσολάβηση τρίτου για τη δημιουργία του ζεύγους κλειδιών ή/και την εγκατάσταση του εγκεκριμένου πιστοποιητικού στην ΕΔΔΥ του συνδρομητή.
   β) Ο πάροχος οφείλει να παρέχει αναλυτικό οδηγό χρήσης της υπηρεσίας και τηλεφωνική γραμμή υποστήριξης δωρεάν, τουλάχιστον για 8 ώρες την ημέρα και 5 ημέρες την εβδομάδα, για την καθοδήγηση του συνδρομητή στα βήματα που απαιτούνται από τη διαδικασία.

Άρθρο 12

Διάρκεια ισχύος εγκεκριμένου πιστοποιητικού

1. Η ημερομηνία και ώρα λήξης ενός εγκεκριμένου πιστοποιητικού δεν μπορεί να υπερβαίνει την ημερομηνία και ώρα λήξης του πιστοποιητικού της Αρχής Πιστοποίησης που έχει χρησιμοποιηθεί για την έκδοσή του.
2. Η διάρκεια ισχύος ενός εγκεκριμένου πιστοποιητικού δεν μπορεί να υπερβαίνει τη διάρκεια χρήσης των αποδεκτών αλγορίθμων δημιουργίας ζεύγους κλειδιών και συναρτήσεων κατακερματισμού, στους οποίους βασίζεται, όπως ορίζονται στην παρ. 1 του άρθρου 14 της παρούσας.

Commented [A13]: Οι ΠΥΕ είναι υπεύθυνοι για την ασφαλή παράδοση των δεδομένων δημιουργίας υπογραφής στους δικαιούχους. Αυτά είναι τα δεδομένα που μπορούν να προκαλέσουν τη δημιουργία μιας εγκεκριμένης ή προηγμένης ηλεκτρονικής υπογραφής. Ένα πιστοποιητικό μπορεί να εκδοθεί μια χρονική στιγμή αλλά δεν μπορεί να χρησιμοποιηθεί από τον δικαιούχο μέχρι να παραλάβει τα δεδομένα δημιουργίας υπογραφής. Συνεπώς, αν ο ΠΥΕ λάβει κατάλληλα μέτρα ώστε να παραδώσει με ασφάλεια τα δεδομένα δημιουργίας υπογραφής στον δικαιούχο, δεν υπάρχει επίπτωση στην ασφάλεια των συναλλαγών αν το συσχετιζόμενο πιστοποιητικό έχει ημερομηνία έναρξης πριν την παράδοση των δεδομένων δημιουργίας υπογραφής. Η συγκεκριμένη πρόταση είναι προβληματική και δημιουργεί εμπόδια στη λειτουργία των ΠΥΕ που ακολουθούν γνωστές και διεθνώς αποδεκτές πρακτικές για τη δημιουργία, αποστολή και ενεργοποίηση των δεδομένων δημιουργίας υπογραφής.

Προτείνεται να επαναδιατυπωθεί ως εξής:
«Τα δεδομένα δημιουργίας υπογραφής που αντιστοιχούν σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής ή σφραγίδας, πρέπει να βρίσκονται στην αποκλειστική κατοχή των νόμιμων κατόχων τους μετά τη δημιουργία και παράδοσή τους από τον ΠΥΕ, και σε καμία περίπτωση δεν επιτρέπεται να βρίσκονται στην κατοχή κάποιου τρίτου μέρους κατά τη διάρκεια ισχύος του εγκεκριμένου πιστοποιητικού».

Commented [A14]: Για λόγους ομοιομορφίας και συνέπειας με την ορολογία του Κανονισμού, «το ζεύγος κλειδιών» προτείνεται να αλλάξει σε «τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής»

Commented [A15]: Εκτός του ότι η συγκεκριμένη πρόταση είναι ιδιαίτερα μεγάλη και δυσνόητη, δεν υποστηρίζει όλες οι διεθνώς αποδεκτές πρακτικές όπως για παράδειγμα τη δημιουργία δεδομένων δημιουργίας υπογραφής από τον ΠΥΕ εντός των ΕΔΔΥ και εκ των υστέρων χρήση τους για έκδοση εγκεκριμένου πιστοποιητικού συνδέοντας τα δεδομένα δημιουργίας υπογραφής με συγκεκριμένη ταυτότητα. ...

Commented [A16]: Υπάρχουν πιο μοντέρνες τεχνικές με "**short-term certificates**" (βλ. ETSI TSP πρότυπα) που δεν υποστηρίζονται από το Άρθρο 11 και γενικότερα από το κείμενο της ΥΑ. Προτείνεται να εξεταστεί το σύνολο της εισήγησης λαμβάνοντας υπ' όψιν το μοντέλο αυτό και να εξασφαλισθεί η συμβατότητα της ΥΑ με τη συγκεκριμένη πρακτική που χρησιμοποιείται ήδη διεθνώς.

Commented [A17]: Σε τεχνικό επίπεδο, μπορεί να παρατηρούνται μικρές χρονικές αποκλίσεις λόγω γνωστού προβλήματος στο Διαδίκτυο με το συγχρονισμό ώρας σε υπολογιστές συνδρομητών και βασιζόμενων μερών. Συνηθίζεται να υπάρχει απόκλιση μέχρι και μερικές ώρες πίσω ώστε ο συνδρομητής που πιθανός να έχει απόκλιση να μπορεί να χρησιμοποιήσει το πιστοποιητικό του με την παραλαβή. ...

Commented [A18]: Δεν είναι κατανοητό πώς μπορεί να εφαρμοσθεί αυτή η διάταξη ούτε πώς σχετίζεται με το Άρθρο 12, παρ. 1 το οποίο αναφέρεται για πιστοποιητικά με ημερομηνία/ώρα λήξης πέρα από την ημερομηνία/ώρα λήξης της ΑΠ που τα έχει εκδώσει.

Προτείνεται η αφαίρεση της παραγράφου.

Commented [A19]: Εκτιμούμε ότι ο συνδρομητής και ο ΠΥΕ είναι το «πρώτο» και «δεύτερο» μέρος αντίστοιχα, τα οποία επιτρέπεται να δημιουργούν δεδομένα δημιουργίας υπογραφής. Παρακαλούμε να διευκρινισθεί για μεγαλύτερη σαφήνεια.

Επιπλέον, αν αξιοποιηθεί κάποιος πιστοποιημένος συνεργάτης του ΠΥΕ λειτουργώντας υπό την καθοδήγηση του ΠΥΕ και παρέχοντ ...

Commented [A20]: Δεδομένων δημιουργίας υπογραφής

Commented [A21]: Κάθε ΠΥΕ οφείλει να παρέχει υπηρεσίες στους συνδρομητές του καθώς και την απαραίτητη τεχνική υποστήριξη. Σε περίπτωση που ένας ΠΥΕ δεν παρέχει ικανοποιητικό επίπεδο υποστήριξης (οδηγούς χρήσης, τηλ. υποστήριξη) ο συνδρομητής μπορεί να ζητήσει τα χρήματά του πίσω και να απευθυνθεί σε άλλο ΠΥΕ. Το επίπεδο εξυπηρέτησης είναι ...

Άρθρο 13

Χρόνος υπογραφής κατά την επικύρωση (άρθρα 32 και 40 Κανονισμού eIDAS)

1. Κατά την επικύρωση εγκεκριμένης ηλεκτρονικής υπογραφής ή σφραγίδας χρησιμοποιείται αξιόπιστη πηγή που βεβαιώνει το χρόνο υπογραφής του εγγράφου (π.χ. εγκεκριμένη χρονοσφραγίδα, πρότυπο ETSI TS 119 102-1, στην εκάστοτε ισχύουσα έκδοσή του). Απουσία αξιόπιστης πηγής, η επικύρωση γίνεται στον τρέχοντα χρόνο.
2. Για την επικύρωση εγγράφων, που έχουν καταχωριστεί σε ηλεκτρονικό πρωτόκολλο δημόσιου φορέα, στο οποίο αποθηκεύεται και αντίγραφο του εγγράφου σε ηλεκτρονική μορφή, μπορεί, εφόσον δεν υπάρχει άλλη αξιόπιστη πηγή που βεβαιώνει το χρόνο υπογραφής, να χρησιμοποιηθεί η ημερομηνία και ώρα πρωτοκόλλησης. Στην περίπτωση αυτή, η έκδοση του εγγράφου που χρησιμοποιείται για τον έλεγχο της εγκυρότητας των υπογραφών, είναι αυτή που έχει καταχωριστεί στο ηλεκτρονικό πρωτόκολλο της υπηρεσίας.
3. Τα αναφερόμενα στις ανωτέρω δύο παραγράφους εφαρμόζονται κατά τον έλεγχο της εγκυρότητας κάθε υπογραφής ή σφραγίδας στο έγγραφο ξεχωριστά.
4. Ανεξάρτητα του τρόπου με τον οποίο προκύπτει ο χρόνος υπογραφής του εγγράφου, εφαρμόζονται κατά την επικύρωση οι περιορισμοί στη χρήση αλγορίθμων κρυπτογράφησης που αναφέρονται στο άρθρο 14 της παρούσας, όπως αυτοί ισχύουν, τη στιγμή που γίνεται η επικύρωση. Η εγκεκριμένη υπηρεσία διαφύλαξης ηλεκτρονικών υπογραφών και σφραγίδων μπορεί να χρησιμοποιηθεί προκειμένου οι υπηρεσίες επικύρωσης να εξακολουθούν να διακριβώνουν τις εγκεκριμένες υπογραφές ή σφραγίδες σε ένα έγγραφο ως έγκυρες ακόμα και όταν οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιήθηκαν σε αυτές παύουν να θεωρούνται ασφαλείς, κατά τα οριζόμενα στο άρθρο 14, παρ. 1.

Μέρος Γ' : Θέματα αλγορίθμων δημιουργίας ζεύγους κλειδιών και συναρτήσεων κατακερματισμού (hash functions)

Άρθρο 14

Αποδεκτοί αλγόριθμοι δημιουργίας ζεύγους κλειδιών και συναρτήσεων κατακερματισμού

1. Οι αποδεκτοί αλγόριθμοι δημιουργίας ζεύγους κλειδιών και συναρτήσεων κατακερματισμού είναι αυτοί που αναφέρονται στο πρότυπο ETSI TS 119 312, στην εκάστοτε ισχύουσα έκδοσή του, με τους περιορισμούς που αναφέρονται σε αυτό.
2. Κατά παρέκκλιση των ανωτέρω, ο αλγόριθμος κατακερματισμού SHA-1 γίνεται δεκτός έως και την 1-6-2022. Μετά την ημερομηνία αυτή, απαγορεύεται η χρήση του για την παροχή οποιασδήποτε υπηρεσίας εμπιστοσύνης, εγκεκριμένης και μη. Η ΕΕΤΤ οφείλει να προχωρήσει στην κατάλληλη ενημέρωση του Καταλόγου Υπηρεσιών Εμπιστοσύνης, αποσύροντας το καθεστώς της «εγκεκριμένης» από κάθε εγκεκριμένη υπηρεσία της οποίας ένα ή περισσότερα στοιχεία χρησιμοποιούν το συγκεκριμένο αλγόριθμο κατακερματισμού.

Άρθρο 15

Εποπτεία και Κυρώσεις

Η συμμόρφωση με τις διατάξεις της παρούσας εποπτεύεται από την ΕΕΤΤ.

Commented [A22]: Δεν ορίζεται ποια είναι η «αξιόπιστη πηγή». Για παράδειγμα, η «ώρα του υπολογιστή» ή μια «μη εγκεκριμένη χρονοσφραγίδα» που ενσωματώνεται στην ηλεκτρονική υπογραφή θεωρείται από την ΕΕΤΤ ως «αξιόπιστη πηγή»; Παρακαλούμε να διευκρινισθεί η κάθε περίπτωση. Ιδανικά, θα πρέπει να δοθεί λίστα με τις αποδεκτές ως «αξιόπιστες» πηγές διότι η συγκεκριμένη διάταξη μπορεί να δημιουργήσει επιπλοκές και σε νομικό επίπεδο (π.χ. διαγωνισμούς, συμβάσεις, κ.α.).

Commented [A23]: Σημειώνουμε ότι πρόκειται για μια λύση που δεν δύναται να εφαρμοστεί χωρίς να προκύψουν κενά ασφάλειας. Το «ηλεκτρονικό πρωτόκολλο» δημόσιου φορέα δεν έχει συγκεκριμένες τεχνικές προδιαγραφές ούτε εγγυήσεις ως προς την αξιοπιστία του. Πολλά ηλεκτρονικά πρωτόκολλα δημόσιων φορέων επιτρέπουν τροποποιήσεις καταχωρήσεων μέσω βάσεων δεδομένων με αποτέλεσμα να είναι εύκολη η αλλαγή των τιμών.

Commented [A24]: Χρειάζεται διευκρίνιση αν στον έλεγχο επικύρωσης πρέπει να ελεγχθεί ότι οι αλγόριθμοι του άρθρου 14 ισχύουν **τη στιγμή της επικύρωσης** ή **τη στιγμή της εκτιμώμενης υπογραφής του εγγράφου**.

Για παράδειγμα, αν γίνει έλεγχος μιας υπογραφής στις 1-7-2022 ενός εγγράφου που είχε εκτιμώμενη δημιουργία υπογραφής στις 1-7-2021 με SHA1 και φέρει εγκεκριμένη χρονοσήμανση 1-7-2021 επίσης με SHA1, θα επικυρωθεί με επιτυχία ή θα θεωρηθεί άκυρη;

Επίσης, τι θα ισχύει αν η SHA1 υπογραφή δεν φέρει εγκεκριμένη χρονοσήμανση αλλά χρονοσήμανση από την ημερομηνία/ώρα του υπολογιστή του υπογράφοντα; Θα επικυρωθεί με επιτυχία ή θα θεωρηθεί άκυρη;

Τέλος, αν γίνει έλεγχος μιας υπογραφής στις 1-7-2022 ενός εγγράφου που είχε εκτιμώμενη δημιουργία υπογραφής στις 1-7-2021 με SHA1 και φέρει εγκεκριμένη χρονοσήμανση 1-7-2021 επίσης με SHA1, και νεότερη εγκεκριμένη χρονοσήμανση SHA256 στις 1-8-2021, θα επικυρωθεί με επιτυχία ή θα θεωρηθεί άκυρη; Αν επικυρωθεί με επιτυχία, ποια θα θεωρείται η πιο αξιόπιστη ημερομηνία υπογραφής του εγγράφου;

Commented [A25]: Η συγκεκριμένη διατύπωση αφορά μόνο τον ΠΥΕ και τη χρήση των SHA1 πιστοποιητικών Αρχής Πιστοποίησης για την έκδοση νέων πιστοποιητικών. Το πρόβλημα εμπιστοσύνης του αλγόριθμου SHA1 δεν περιορίζεται μόνο στην Αρχή Πιστοποίησης αλλά και στους τελικούς συνδρομητές.

Να διευκρινιστεί τι ισχύει για τους κατόχους πιστοποιητικού εγκεκριμένης ηλεκτρονικής υπογραφής με SHA1. Προφανώς, οι συγκεκριμένοι κάτοχοι πρέπει να σταματήσουν να υπογράφουν έγγραφα από 2/6/2022 με τα συγκεκριμένα πιστοποιητικά προκειμένου να μη δημιουργηθεί πρόβλημα εμπιστοσύνης. Ιδανικά, όλα τα πιστοποιητικά αυτά θα πρέπει να ανακληθούν από τους ΠΥΕ μέχρι τις 2/6/2022.

Σε περίπτωση διαπίστωσης παράβασης των διατάξεων της παρούσας, η ΕΕΤΤ, με ειδικά αιτιολογημένη απόφασή της και ύστερα από προηγούμενη ακρόαση των ενδιαφερομένων. δύναται να επιβάλει τις διοικητικές κυρώσεις του άρθρου 56 του Ν. 4727/2020.

ΜΕΡΟΣ Β

ΠΡΟΤΕΙΝΟΜΕΝΟ ΠΕΡΙΕΧΟΜΕΝΟ

Υπουργικής Απόφασης άρθρου 107 παρ. 34 του ν.4727/2020

Άρθρο 9

Σκοπός και πεδίο εφαρμογής

Σκοπός της παρούσας είναι η ρύθμιση ειδικότερων ζητημάτων των υπηρεσιών εμπιστοσύνης και, συγκεκριμένα, θεμάτων που αφορούν στην ανάκληση εγκεκριμένων πιστοποιητικών.

Για τους σκοπούς της παρούσας ισχύουν οι ορισμοί του άρθρου 3 του Κανονισμού (ΕΕ) 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ.

Άρθρο 10

Ενημέρωση κατάστασης εγκεκριμένων πιστοποιητικών

1. Συστήνεται η υλοποίηση Ηλεκτρονικού ή Επιγραμμικού Πρωτοκόλλου Κατάστασης Πιστοποιητικού (Online Certificate Status Protocol - OCSP) για την ενημέρωση των Βασιζόμενων Μερών (Relying Parties) σχετικά με την κατάσταση ενός εγκεκριμένου πιστοποιητικού. Εάν ο Πάροχος Υπηρεσιών Εμπιστοσύνης (ΠΥΕ) επιλέξει να μην υλοποιήσει το OCSP πρωτόκολλο τότε υποχρεούται στη δημοσίευση Λίστας Ανακληθέντων Πιστοποιητικών (Certificate Revocation List – CRL).
2. Όταν ο ΠΥΕ παρέχει την πληροφορία σχετικά με την κατάσταση των εκδοθέντων από αυτόν εγκεκριμένων πιστοποιητικών μέσω OCSP και CRL, εφαρμόζονται οι διατάξεις του προτύπου ETSI EN 319-412-2 σχετικά με τη συνάφεια της πληροφορίας που παρέχεται μέσω των δύο τρόπων ενημέρωσης. Η συμμόρφωση με την απαίτηση αυτή κατά την υλοποίηση του OCSP δεν αποκλείει τη χρήση της κατάστασης “unknown” ή “revoked” στην περίπτωση υποβολής ερωτήματος για άγνωστο πιστοποιητικό, σύμφωνα με την ενότητα 2.2 του RFC6960.

Άρθρο 11

Διαθεσιμότητα της κατάστασης ενός ανακληθέντος πιστοποιητικού μετά τη λήξη του

1. Ο ΠΥΕ εξασφαλίζει ότι η πληροφορία σχετικά με την κατάσταση ενός ανακληθέντος εγκεκριμένου πιστοποιητικού παραμένει διαθέσιμη μέσω OCSP ή/και CRL και μετά τη λήξη του πιστοποιητικού.
2. Για τη συμμόρφωση με την υποχρέωση της ανωτέρω παραγράφου, εφαρμόζονται τα ακόλουθα:
   α. Μετά τη λήξη ενός εγκεκριμένου πιστοποιητικού: (i) αν ο ΠΥΕ δημοσιεύει CRL τότε πρέπει να περιλαμβάνεται η επέκταση “ExpiredCertsOnCRL” και να ακολουθούν οι σειριακοί αριθμοί όλων των ανακληθέντων πιστοποιητικών, ακόμα και αυτών που έληξαν αφού πρώτα ανακλήθηκαν και (ii) αν ο ΠΥΕ υλοποιεί OCSP τότε πρέπει να περιλαμβάνεται η επέκταση “archive cutoff” (RFC6960) με

Commented [A26]: Με τη συγκεκριμένη διατύπωση, δεν υποστηρίζεται η αποδεκτή και ασφαλής λύση των μικρής διάρκειας “short-term” πιστοποιητικών, σύμφωνα με τα ETSI EN 319 411-2, 411-1, 412-1, τα οποία επειδή είναι μικρής διάρκειας δεν απαιτείται να έχουν πληροφορίες κατάστασης εγκυρότητας. Ακόμα κι αν ο ΠΥΕ υποστηρίζει τις εν λόγω υπηρεσίες CRL ή/και OCSP, για τη συγκεκριμένη κατηγορία πιστοποιητικών (Short-term) δεν απαιτείται να έχουν πληροφορίες κατάστασης. Επίσης, τα εν λόγω πιστοποιητικά δεν μπορούν να ανακληθούν (βλ. απαίτηση **REV-6.3.9-15** στο ETSI EN 319 411-1).

Προτείνεται η τροποποίηση της παραγράφου (ενδεχομένως και άλλων σημείων) ώστε να λαμβάνει υπ’ όψιν τη συγκεκριμένη πρακτική που εφαρμόζεται από πολλούς εγκεκριμένους ΠΥΕ στην Ευρωπαϊκή Ένωση.

Commented [A27]: 319 411-2, το οποίο παραπέμπει στο 319 411-1 (υποθέτουμε ότι η αναφορά γίνεται για την **CSS-6.3.10-09** του 319 411-1)

Commented [A28]: Συστήνουμε να γίνει υποχρεωτική η απάντηση “Unknown” ή “revoked” ως απάντηση των OCSP responders για άγνωστα πιστοποιητικά προκειμένου να αντιμετωπισθούν γνωστοί κίνδυνοι. Για περισσότερες πληροφορίες, δείτε την απαίτηση **OVR-6.6.3-02** από το ETSI EN 319 411-1.

Commented [A29]: Δεν είναι τεχνικά εφικτό να υπάρχει η συγκεκριμένη επέκταση σε όλες τις περιπτώσεις OCSP responses (ειδικά μέσω τεχνικών pre-signed responses). Τα ETSI πρότυπα το έχουν ως «σύσταση» και όχι ως υποχρεωτική απαίτηση (ETSI EN 319 411-2 CSS-6.3.10-10). Προτείνεται να αλλάξει το «πρέπει» σε «συστήνεται» για να ταιριάζει με το “SHOULD” από τα πρότυπα. Σημειώνεται ότι και στο RFC 6960 η επέκταση αυτή αναφέρεται ως “SHOULD”.

Θεωρούμε πιο σημαντικό να ρυθμιστούν οι OCSP responders να ΜΗΝ επιστρέφουν απάντηση κατάστασης “good” σε άγνωστα πιστοποιητικά.

ημερομηνία αυτή της έναρξης του πιστοποιητικού της Αρχής Πιστοποίησης (Certificate Authority – CA, σύμφωνα με το πρότυπο ETSI EN 319 411-2) και να ενημερώνει για την κατάσταση κάθε ανακληθέντος πιστοποιητικού και μετά τη λήξη του.

β. Αν το πιστοποιητικό μιας εκδότριας Αρχής Πιστοποίησης (CA) πρόκειται να λήξει τότε (i) ο ΠΥΕ ανακαλεί όλα τα εκδοθέντα από αυτήν την Αρχή Πιστοποίησης πιστοποιητικά με ημερομηνία λήξης μετά τη λήξη του πιστοποιητικού της CA, (ii) αν ο ΠΥΕ δημοσιεύει CRL τότε μια τελική CRL πρέπει να εκδοθεί με ημερομηνία λήξης την 31 Δεκεμβρίου 9999, 23:59:59 (“99991231235959Z”) και (iii) αν ο ΠΥΕ υλοποιεί OCSP τότε μια τελική απάντηση OCSP πρέπει να είναι διαθέσιμη για κάθε εκδοθέν πιστοποιητικό με ημερομηνία λήξης της απάντησης αυτής την 31 Δεκεμβρίου 9999, 23:59:59 (“99991231235959Z”).

γ. Αν ο ΠΥΕ σταματήσει την παροχή μιας εγκεκριμένης υπηρεσίας, χωρίς να τη μεταφέρει σε άλλο εγκεκριμένο πάροχο τότε εφαρμόζονται οι προβλέψεις της ανωτέρω β΄ παραγράφου. Επιπλέον, ο ΠΥΕ δεν υποχρεούται στη συνέχιση της δημοσίευσης CRL ή τη διατήρηση της υπηρεσίας OCSP για τις Αρχές Πιστοποίησης (CAs) της καταργηθείσας υπηρεσίας αλλά πρέπει να διασφαλίζει ότι η τελική CRL ή/και οι τελικές απαντήσεις OCSP παραμένουν διαθέσιμες στα Βασιζόμενα Μέρη.

δ. Ο ΠΥΕ ενημερώνει κατάλληλα τα συστήματά του για όλα τα πιστοποιητικά που έχουν λήξει ή ανακληθεί, στο βαθμό που αυτό είναι εφικτό, και ανεξαρτήτως του αν ο χρόνος έκδοσής τους προηγείται της έναρξης ισχύος της παρούσας.

3. Σε κάθε περίπτωση, ο ΠΥΕ δημοσιεύει κατάλληλα τον τρόπο συμμόρφωσης με την απαίτηση του παρόντος άρθρου.

Commented [A30]: Αναφέρεται σε πιστοποιητικά που λήγουν μετά την λήξη της ΑΠ που τα εξέδωσε, γεγονός που είναι ασύμβατο με το Μέρος Α' Άρθρο 12.1. Επιπλέον, σύμφωνα με τον αλγόριθμο επαλήθευσης του RFC 5280, ένα πιστοποιητικό δεν μπορεί να θεωρείται έγκυρο μετά την λήξη της αρχής που το εξέδωσε, συνεπώς πρόκειται για παράβαση διεθνούς προτύπου.

Commented [A31]: ΠΥΕ

Commented [A32]: Να διευκρινιστεί πώς μπορεί να εφαρμοστεί πρακτικά αυτή η διάταξη όταν ο ΠΥΕ σταματήσει την παροχή υπηρεσίας και «δεν υποχρεούται στη συνέχιση της δημοσίευσης CRL ή τη διατήρηση της υπηρεσίας OCSP».

Commented [A33]: Δεν είναι κατανοητό το περιεχόμενο αυτής της παραγράφου. Τι ακριβώς προσπαθεί να διασφαλίσει και ποια είναι ακριβώς η απαίτηση-σύσταση;

Commented [A34]: Για να μην υπάρχει παρανόηση καθώς και για λόγους διαφάνειας, είναι σκόπιμο να ορισθεί το CP/CPS ως το κατάλληλο σημείο όπου ο ΠΥΕ θα περιγράφει τον τρόπο συμμόρφωσης με τις απαιτήσεις του παρόντος άρθρου.

Commented [A35]: Από τη στιγμή που είναι παραπάνω από μία απαιτήσεις, προτείνεται να διορθωθεί με «τις απαιτήσεις» του παρόντος άρθρου.