Μαρούσι, 24-5-2022
ΑΠ 1031/4

ΑΠΟΦΑΣΗ

Υποβολή Πρότασης προς τον Υπουργό Ψηφιακής Διακυβέρνησης σύμφωνα με τα προβλεπόμενα στο άρθρο 107, παρ. 31 και 34 του Ν. 4727/2020, για την έκδοση υπουργικής απόφασης για τη ρύθμιση ειδικότερων ζητημάτων της παροχής εγκεκριμένων υπηρεσιών εμπιστοσύνης και της ανάκλησης εγκεκριμένων πιστοποιητικών

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)

Έχοντας υπόψη :

α. Το Ν. 4727/2020 (ΦΕΚ 184/Α/23-9-2020) «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις», ιδίως τις διατάξεις των άρθρων 107 παρ. 31 και 34, 131 και 48-58 αυτού,

β. Το Ν. 4070/2012 (ΦΕΚ 82/Α/10-4-2012) «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις», όπως ισχύει, ιδίως το άρθρο 12 παρ. 1 περ. κε' αυτού, όπως τροποποιήθηκε με το άρθρο 108 παρ. 7 του Ν. 4727/2020 (ΦΕΚ Α' 184/23-9-2021),

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

δ. Την Υπουργική Απόφαση 27499ΕΞ2021 (ΦΕΚ 3682 Β΄/10-8-2021) «Πρότυπα και απαιτήσεις για τη μέθοδο εξ αποστάσεως ταυτοποίησης φυσικών προσώπων, με σκοπό την έκδοση πιστοποιητικού υπηρεσίας εμπιστοσύνης»,

ε. Την Απόφαση της ΕΕΤΤ ΑΠ 837/1Β/30-11-2017 «Κανονισμός Παροχής Υπηρεσιών Εμπιστοσύνης» (ΦΕΚ 4396/Β΄/14-12-2017),

στ. Την Απόφαση της ΕΕΤΤ ΑΠ 375/10/14-2-2006, «Κανονισμός Διαδικασίας Δημόσιας Διαβούλευσης» (ΦΕΚ 314/Β/16.03.2006),

ζ. Την Απόφαση της ΕΕΤΤ ΑΠ 1016/5/22-11-2021 «Διεξαγωγή δημόσιας διαβούλευσης σχετικά με τη ρύθμιση ειδικότερων ζητημάτων της παροχής εγκεκριμένων υπηρεσιών εμπιστοσύνης και ανάκλησης εγκεκριμένων πιστοποιητικών, με σκοπό την υποβολή εισήγησης προς τον Υπουργό Ψηφιακής Διακυβέρνησης κατ' άρθρο 107 παρ. 31 και 34 Ν. 4727/2020»,

η. Τη Δημόσια διαβούλευση που διενήργησε η ΕΕΤΤ από 25-11-2021 μέχρι 17-12-2021,

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

θ. Τα σχόλια που υποβλήθηκαν στο πλαίσιο της διενεργηθείσας δημόσιας διαβούλευσης από τις ακόλουθες εταιρείες/ τους ακόλουθους παρόχους υπηρεσιών εμπιστοσύνης:

- «ΑΝΤΑΚΟΜ – ΠΡΟΗΓΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ ΔΙΑΔΙΚΤΥΟΥ Α.Ε. (ADACOM S.A.)»
- «HELLENIC EXCHANGES - ATHENS STOCK EXCHANGE SA (ATHEX)»
- «BYTE Computer ΑΒΕΕ»
- «ΑΚΑΔΗΜΑΪΚΟ ΔΙΑΔΙΚΤΥΟ (GUnet)»
- «QMSCert»

ι. Την υπ' αρ. πρωτ. 29984/10-11-2021 επιστολή της ΕΕΤΤ προς τον κ. Υπουργό Ψηφιακής Διακυβέρνησης, αναφορικά με την «Κατάργηση της δυνατότητας αναστολής της ισχύος εγκεκριμένων πιστοποιητικών υπηρεσιών εμπιστοσύνης – τροποποίηση άρθρου 54 ν.4727/2020»,

ια. Την Απόφαση της ΕΕΤΤ ΑΠ 1031/1/24-5-2022 «Έγκριση των αποτελεσμάτων δημόσιας διαβούλευσης της ΕΕΤΤ σχετικά με τη ρύθμιση ειδικότερων ζητημάτων της παροχής εγκεκριμένων υπηρεσιών εμπιστοσύνης και της αναστολής ισχύος και ανάκλησης εγκεκριμένων πιστοποιητικών»,

ιβ. Τα επισυναπτόμενα στο παράρτημα της παρούσας Απόφασης κείμενα υπό τους τίτλους: 1) «Πρόταση της ΕΕΤΤ για την έκδοση Υ.Α. σύμφωνα με τα προβλεπόμενα στο άρθρο 107 παρ. 31 Ν. 4727/2020» και 2) «Πρόταση της ΕΕΤΤ για την έκδοση Υ.Α. σύμφωνα με τα προβλεπόμενα στο άρθρο 107 παρ. 34 Ν. 4727/2020»,

ια. Την υπ΄ αρ. πρωτ. 36091/19-5-2022 εισήγηση της αρμόδιας υπηρεσίας της ΕΕΤΤ και κατόπιν προφορικής εισήγησης του Προέδρου, Καθηγ. Κων/νου Μασσέλου και του Αντιπροέδρου, Καθηγ. Δημ. Βαρουτά.

Αποφασίζει:

Εγκρίνει την υποβολή Πρότασης προς τον Υπουργό Ψηφιακής Διακυβέρνησης, σύμφωνα με τα προβλεπόμενα στο άρθρο 107 παρ. 31 και 34 Ν. 4727/2020 (ΦΕΚ Α' 184/23.09.2020), για την έκδοση υπουργικών αποφάσεων αναφορικά με τη ρύθμιση ειδικότερων ζητημάτων της παροχής εγκεκριμένων υπηρεσιών εμπιστοσύνης και της ανάκλησης εγκεκριμένων πιστοποιητικών, σύμφωνα με τα κείμενα που επισυνάπτονται ως παράρτημα της παρούσας υπό τους τίτλους: «Πρόταση της ΕΕΤΤ για την έκδοση Υ.Α. σύμφωνα με τα προβλεπόμενα στο άρθρο 107 παρ. 31 Ν. 4727/2020» και «Πρόταση της ΕΕΤΤ για την έκδοση Υ.Α. σύμφωνα με τα προβλεπόμενα στο άρθρο 107 παρ. 34 Ν. 4727/2020».

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

ΠΑΡΑΡΤΗΜΑ

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

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

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

Άρθρο 3

Αριθμός μητρώου εγκεκριμένου ΠΥΕ (Παραρτήματα Ι, σημείο β, ΙΙΙ, σημείο β και IV, σημείο β)

1. Ο αριθμός μητρώου του εγκεκριμένου ΠΥΕ, που περιλαμβάνεται στα εγκεκριμένα πιστοποιητικά που εκδίδει, όπως ορίζεται στα Παραρτήματα Ι, ΙΙΙ και IV του Κανονισμού eIDAS, δηλώνεται στο χαρακτηριστικό "organizationIdentifier" του πεδίου Εκδότης (Issuer) σύμφωνα με τα οριζόμενα στο πρότυπο ETSI EN 319 412-1, στην εκάστοτε ισχύουσα έκδοσή του. Κατ' εξαίρεση, στην περίπτωση των προθεμάτων "TIN" και "VAT", όπου αυτά χρησιμοποιούνται, γίνεται ισχυρή σύσταση να χρησιμοποιείται ο κωδικός χώρας "EL" αντί του κωδικού "GR".

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>. Στην περίπτωση αυτή, θα περιλαμβάνεται στα τελικά εγκεκριμένα πιστοποιητικά το στοιχείο "nameRegistrationAuthorities" της Δήλωσης Εγκεκριμένου Πιστοποιητικού (QC Statement) "SemanticsInformation" (IETF RFC 3739) και θα περιέχει ένα πεδίο "generalName" με τιμή:

   https://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/EsignProviders.html.

3. Ειδικά για τις Αρχές Πιστοποίησης που είναι ήδη εγκεκριμένες κατά την έναρξη ισχύος της παρούσας και δεν περιλαμβάνουν στα εκδιδόμενα εγκεκριμένα πιστοποιητικά τον αριθμό μητρώου του εγκεκριμένου ΠΥΕ στο πεδίο Εκδότης (Issuer), δύνανται να τον συμπεριλάβουν σε άλλο πεδίο με κατάλληλη διατύπωση (π.χ. "Issued by QTSP … with VATEL-…").

4. Κάθε ΠΥΕ υποχρεούται να ανακαλέσει όλα τα ήδη εκδοθέντα εγκεκριμένα πιστοποιητικά στα οποία δεν περιλαμβάνεται ο αριθμός μητρώου του, σύμφωνα με τα παραπάνω, εντός ενός (1) μηνός από την έναρξη ισχύος της παρούσας.

5. 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 4

Αριθμός μητρώου του δημιουργού εγκεκριμένης ηλεκτρονικής σφραγίδας (Παράρτημα ΙΙΙ, σημείο γ)

1. Ο αριθμός μητρώου του δημιουργού μιας εγκεκριμένης ηλεκτρονικής σφραγίδας, που περιλαμβάνεται στο πεδίο Υποκείμενο (Subject) του εγκεκριμένου πιστοποιητικού, όπως ορίζεται στο Παράρτημα ΙΙΙ του Κανονισμού eIDAS, δηλώνεται στο χαρακτηριστικό "organizationIdentifier" σύμφωνα με τα οριζόμενα στο πρότυπο ETSI EN 319 412-1, στην εκάστοτε ισχύουσα έκδοσή του. Κατ' εξαίρεση, στην περίπτωση

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

του προθέματος "VAT", γίνεται ισχυρή σύσταση να χρησιμοποιείται ο κωδικός χώρας "EL" αντί του κωδικού "GR".

Άρθρο 5

Δήλωση ονόματος κατόχου και Χρήση ψευδωνύμων (Παραρτήματα I και IV)

1. Το όνομα του φυσικού προσώπου, στο οποίο έχει εκδοθεί το εγκεκριμένο πιστοποιητικό, δηλώνεται κατάλληλα στα στοιχεία "surname" (επώνυμο, OID 2.5.4.4) και "givenName" (όνομα, OID 2.5.4.42) στο πεδίο Υποκείμενο (Subject) του εγκεκριμένου πιστοποιητικού και πρέπει να ταυτίζεται με το ονοματεπώνυμο που περιλαμβάνεται στο έγγραφο ταυτοποίησης που χρησιμοποιήθηκε κατά την ταυτοποίησή του.
2. 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. Στην περίπτωση αυτή, δεν επιτρέπεται να περιλαμβάνονται στο εγκεκριμένο πιστοποιητικό τα στοιχεία "surname" και "givenName" στο πεδίο Υποκείμενο. Η διαδικασία με την οποία ο πάροχος ελέγχει και επιβεβαιώνει το ψευδώνυμο του φυσικού προσώπου κατά την έκδοση εγκεκριμένου πιστοποιητικού, πιστοποιείται από κατάλληλο Οργανισμό Αξιολόγησης Συμμόρφωσης.

Άρθρο 6

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.
3. Το περιεχόμενο των τελικών πιστοποιητικών για την επαλήθευση της γνησιότητας ιστοτόπου ακολουθεί τα οριζόμενα στο πρότυπο ETSI EN 319 412-4, στην εκάστοτε ισχύουσα έκδοσή του, εκτός από τα σημεία που ορίζεται διαφορετικά στην παρούσα.
4. Οι εγκεκριμένοι ΠΥΕ οφείλουν να συμμορφώνονται με τις προβλέψεις κάθε νέας έκδοσης προτύπου ETSI, που αναφέρεται στις ανωτέρω παραγράφους, εντός έξι (6) μηνών από τη δημοσίευσή της.

Άρθρο 7

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) ή με χρήση των μεθόδων ταυτοποίησης αναγνωρισμένων σε εθνικό επίπεδο που παρέχουν διασφάλιση ισοδύναμη με την φυσική παρουσία (άρθρο 24, παρ. 1, στοιχείο δ) του Κανονισμού eIDAS), η ταυτοποίηση πρέπει να έχει διενεργηθεί εντός ενός (1) έτους πριν την έκδοση.
2. Η ταυτοποίηση με φυσική παρουσία δύναται να αποδεικνύεται με τη βεβαίωση του γνησίου της υπογραφής του φυσικού προσώπου ή του εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου επί της αίτησης έκδοσης του εγκεκριμένου πιστοποιητικού, που γίνεται από οποιαδήποτε αρμόδια Διοικητική Αρχή ή Κέντρο Εξυπηρέτησης Πολιτών με αυτοπρόσωπη παρουσία του υπογράφοντα. Η χρήση εγγράφου εκδοθέντος από την

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

εφαρμογή «Ψηφιακή Βεβαίωση Εγγράφου» δεν δύναται να χρησιμοποιηθεί για το σκοπό αυτό.

3. 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) του Κανονισμού eIDAS, η ταυτοποίηση πρέπει να έχει διενεργηθεί εντός ενός (1) μηνός από την έκδοση.

4. Εφόσον η έκδοση εγκεκριμένου πιστοποιητικού βασίζεται σε ταυτοποίηση η οποία γίνεται εξ αποστάσεως, με τη χρήση μέσων ηλεκτρονικής ταυτοποίησης που πληρούν τις απαιτήσεις του "βασικού" ή "υψηλού" επιπέδου διασφάλισης (άρθρο 24, παρ. 1, στοιχείο β) του Κανονισμού eIDAS), ο πάροχος υπηρεσιών εμπιστοσύνης μπορεί να αποδέχεται μέσα ηλεκτρονικής ταυτοποίησης:

   α) τα οποία έχουν κοινοποιηθεί από ένα Κράτος Μέλος της ΕΕ με τη διαδικασία που ορίζεται στον Κανονισμό eIDAS

   β) τα οποία πληρούν τις απαιτήσεις του βασικού ή υψηλού επιπέδου διασφάλισης

   γ) εφόσον έχει υλοποιήσει τη διασύνδεση με τον ελληνικό «Κόμβο eIDAS» (“eIDAS Node”) και τη σχετική υπηρεσία αυθεντικοποίησης, το αποτέλεσμα της οποίας επιβεβαιώνει τα στοιχεία του αιτούντα.

5. 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.

6. Η μέθοδος που χρησιμοποιήθηκε για την ταυτοποίηση του αιτούντα μπορεί να εμφανίζεται στο τελικό πιστοποιητικό. Σε διαφορετική περίπτωση, ο εγκεκριμένος ΠΥΕ, που εξέδωσε ένα εγκεκριμένο πιστοποιητικό, το οποίο είναι σε ισχύ, υποχρεούται να παρέχει την πληροφορία σχετικά με τη μέθοδο ταυτοποίησης που χρησιμοποίησε για την έκδοσή του, σε άλλον εγκεκριμένο ΠΥΕ, κατόπιν αιτιολογημένου αιτήματος του τελευταίου, το αργότερο εντός πέντε (5) εργασίμων ημερών από την υποβολή του. Κάθε αίτημα λαμβάνει μοναδικό αριθμό αναφοράς, ο οποίος αποστέλλεται στον αιτούντα πάροχο κατά την υποβολή του. Κάθε εγκεκριμένος ΠΥΕ οφείλει να δημοσιεύσει στον ιστότοπό του τη διαδικασία με την οποία δέχεται τέτοιου είδους αιτήματα (π.χ. ηλεκτρονικό ταχυδρομείο ή φόρμα στον ιστότοπό του) εντός έξι (6) μηνών από τη θέση σε ισχύ της παρούσας.

Άρθρο 8

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, επιπλέον των άλλων στοιχείων που υποχρεούνται να τηρούν, τα ακόλουθα:

   α) Όταν πρόκειται για εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής:

      i. Την αίτηση έκδοσης εγκεκριμένου πιστοποιητικού πλήρως συμπληρωμένη με όλα τα απαραίτητα στοιχεία και την ημερομηνία και ώρα υποβολής της. Όταν η ταυτοποίηση του αιτούντα δεν προηγείται της υποβολής της αίτησης τότε η αίτηση

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

μπορεί να υποβάλλεται με οποιοδήποτε τρόπο. Όταν χρησιμοποιείται το αποτέλεσμα προγενέστερης ταυτοποίησης τότε η αίτηση πρέπει να φέρει κατάλληλη βεβαίωση του γνησίου της υπογραφής του αιτούνταή την εγκεκριμένη ηλεκτρονική υπογραφή του, οπότε και συστήνεται η χρήση εγκεκριμένης χρονοσφραγίδας, ή να γίνεται μέσω διαδικασίας που περιλαμβάνει την αυθεντικοποίηση του αιτούντα με δεύτερο παράγοντα (π.χ. αποστολή μοναδικού κωδικού μιας χρήσης στο καταχωρισμένο κινητό του αιτούντα ή χρήση τεχνολογίας τουλάχιστον αντίστοιχης διασφάλισης). Σε κάθε περίπτωση, η αίτηση πρέπει να έχει υποβληθεί σε διάστημα όχι μεγαλύτερο των τριών (3) μηνών πριν από την ημερομηνία έκδοσης του πιστοποιητικού.

ii. Τους όρους χρήσης της υπηρεσίας, όπως ίσχυαν κατά το χρόνο υποβολής της αίτησης, υπογεγραμμένους από τον αιτούντα με την ιδιόχειρη ή εγκεκριμένη ηλεκτρονική υπογραφή του, 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 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 και την ημερομηνία και ώρα υποβολής της. Όταν η ταυτοποίηση του αιτούντα γίνεται μετά την υποβολή της αίτησης τότε η αίτηση πρέπει να υπογράφεται από τον νόμιμο εκπρόσωπο ή τον ειδικά εξουσιοδοτημένο εκπρόσωπο του νομικού προσώπου. Όταν χρησιμοποιείται το αποτέλεσμα προγενέστερης ταυτοποίησης του νόμιμου εκπροσώπου ή του ειδικά εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου τότε η αίτηση πρέπει να φέρει κατάλληλη βεβαίωση του γνησίου της υπογραφής του αιτούντα ή την εγκεκριμένη ηλεκτρονική υπογραφή ή την εγκεκριμένη ηλεκτρονική σφραγίδα του νομικού προσώπου ή να γίνεται μέσω διαδικασίας που περιλαμβάνει την αυθεντικοποίηση του αιτούντα με δεύτερο παράγοντα (π.χ. αποστολή μοναδικού κωδικού μιας χρήσης στο καταχωρισμένο κινητό του αιτούντα ή χρήση τεχνολογίας τουλάχιστον αντίστοιχης διασφάλισης). Σε περίπτωση που υπογράφεται με εγκεκριμένη ηλεκτρονική υπογραφή ή σφραγίζεται με εγκεκριμένη ηλεκτρονική σφραγίδα, συστήνεται η χρήση εγκεκριμένης χρονοσφραγίδας. Σε κάθε περίπτωση, η αίτηση πρέπει να έχει υποβληθεί σε διάστημα όχι μεγαλύτερο των τριών (3) μηνών πριν από την ημερομηνία έκδοσης του πιστοποιητικού.

ii. Τους όρους χρήσης της υπηρεσίας, όπως ίσχυαν κατά το χρόνο υποβολής της αίτησης, υπογεγραμμένους από τον νόμιμο εκπρόσωπο ή τον ειδικά εξουσιοδοτημένο εκπρόσωπο του νομικού προσώπου με την ιδιόχειρη ή εγκεκριμένη ηλεκτρονική υπογραφή του ή σφραγισμένους με την εγκεκριμένη ηλεκτρονική σφραγίδα του νομικού προσώπου, άλλως με αποδοχή τους μέσω κατάλληλης επιλογής στην ιστοσελίδα του παρόχου. Στη δεύτερη και τρίτη περίπτωση συστήνεται η χρήση εγκεκριμένης χρονοσφραγίδας. Στην τελευταία περίπτωση ο ΠΥΕ οφείλει να διασφαλίζει ότι η ημερομηνία και ώρα της αποδοχής καταγράφεται στο αρχείο.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

Άρθρο 9

Απαιτήσεις για τις 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 χρησιμοποιεί τα δεδομένα ηλεκτρονικής υπογραφής ή σφραγίδας (άρθρο 26, παρ. γ του Κανονισμού eIDAS).

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 ή έχει πιστοποιηθεί κατάλληλα (άρθρο 30 του Κανονισμού eIDAS).

γ) Όταν τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας δημιουργούνται από το συνδρομητή χωρίς την επίβλεψη του εγκεκριμένου ΠΥΕ μέσω αυτοματοποιημένης υπηρεσίας απομακρυσμένης εγκατάστασης πιστοποιητικών, που παρέχει:

i. η ΕΔΔΥ πρέπει να υποστηρίζει από τον κατασκευαστή της απομακρυσμένο κρυπτογραφικό έλεγχο του δημιουργηθέντος ιδιωτικού κλειδιού και η δυνατότητα αυτή να χρησιμοποιείται από την υπηρεσία αλλιώς ο εγκεκριμένος ΠΥΕ οφείλει να λαμβάνει κατάλληλα τεχνικά μέτρα ώστε, με εύλογο επίπεδο διασφάλισης, να αναγνωρίζει την ΕΔΔΥ που χρησιμοποιεί ο αιτών, η οποία πρέπει να είναι στον κατάλογο των αποδεκτών ΕΔΔΥ, και

ii. οι όροι χρήσης της υπηρεσίας περιλαμβάνουν την υποχρέωση του αιτούντα να δημιουργεί τα δεδομένα δημιουργία ηλεκτρονικής υπογραφής ή σφραγίδας σε ΕΔΔΥ που αποδέχεται ο εγκεκριμένος ΠΥΕ.

Άρθρο 10

Έκδοση και έναρξη ισχύος εγκεκριμένου πιστοποιητικού

1. Η έκδοση των εγκεκριμένων πιστοποιητικών πρέπει να γίνεται είτε τη στιγμή της παράδοσης της ΕΔΔΥ στο συνδρομητή, οπότε και εγκαθίσταται το εκδοθέν πιστοποιητικό από τον ΠΥΕ, 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, 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 απομακρυσμένης υπογραφής ή σφραγίδας 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. Ο εγκεκριμένος ΠΥΕ οφείλει να ελέγχει και να διασφαλίζει ότι η ημερομηνία και ώρα έναρξης που εισάγεται στο πιστοποιητικό δεν αποκλίνει από τη Συγχρονισμένη Παγκόσμια Ώρα πάνω από δύο ώρες.

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.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

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 των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας στην ΕΔΔΥ του συνδρομητή.

   β) Ο πάροχος οφείλει να παρέχει αναλυτικό οδηγό χρήσης της υπηρεσίας απομακρυσμένης εγκατάστασης πιστοποιητικών και τηλεφωνική γραμμή υποστήριξης δωρεάν, τουλάχιστον για 4 ώρες την ημέρα, τις εργάσιμες ημέρες της εβδομάδας, για την καθοδήγηση του συνδρομητή στα βήματα που απαιτούνται για τη δημιουργία των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας, ή/και την εγκατάσταση του εγκεκριμένου πιστοποιητικού στην ΕΔΔΥ του συνδρομητή.

Άρθρο 11

Διάρκεια ισχύος πιστοποιητικού

1. Η ημερομηνία και ώρα λήξης ενός εγκεκριμένου πιστοποιητικού δεν επιτρέπεται 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 13 της παρούσας.

3. Σε μια ιεραρχία που εκδίδει εγκεκριμένα πιστοποιητικά, η διάρκεια ισχύος των πιστοποιητικών κάθε Αρχής Πιστοποίησης της ιεραρχίας συστήνεται να μην υπερβαίνει τη διάρκεια χρήσης των αποδεκτών αλγορίθμων δημιουργίας ζεύγους κλειδιών και συναρτήσεων κατακερματισμού, στους οποίους βασίζεται, όπως ορίζονται στην παρ. 1 του άρθρου 13 της παρούσας.

Άρθρο 12

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 (εγκεκριμένη χρονοσφραγίδα). Απουσία αξιόπιστης πηγής, ως χρόνος υπογραφής του εγγράφου για την επικύρωση ορίζεται η τρέχουσα ημερομηνία/ώρα κατά την οποία λαμβάνει χώρα η επικύρωση.

2. Για την επικύρωση εγγράφων που έχουν καταχωριστεί σε ηλεκτρονικό πρωτόκολλο δημόσιου φορέα, για το οποίο ισχύουν τα ακόλουθα: α) αποθηκεύεται αντίγραφο του εγγράφου σε ηλεκτρονική μορφή με τρόπο που δεν επιτρέπει τη μεταγενέστερη τροποποίησή του και β) καταχωρίζεται ο αριθμός πρωτοκόλλου, η ημερομηνία και η ώρα πρωτοκόλλησης με τρόπο που δεν επιτρέπει τη μεταγενέστερη τροποποίησή τους, και η πληροφορία αυτή κοινοποιείται στον πολίτη που υπέβαλε το έγγραφο, μπορεί, εφόσον δεν υπάρχει άλλη αξιόπιστη πηγή που βεβαιώνει το χρόνο υπογραφής, να χρησιμοποιηθεί η ημερομηνία και ώρα πρωτοκόλλησης του εγγράφου ως χρόνος υπογραφής για την επικύρωση. 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.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

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 13 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 13, παρ. 1. Στο Παράρτημα Α δίνονται παραδείγματα σχετικά με το πώς επηρεάζεται το αποτέλεσμα της επικύρωσης από την πρόβλεψη της παρούσας παραγράφου.

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

Άρθρο 13

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, έκδοση V1.4.2, με τους περιορισμούς που αναφέρονται σε αυτό. Στην περίπτωση που μια νέα έκδοση του προτύπου ETSI TS 119 312 καθιστά ένα αλγόριθμο μη αποδεκτό, με Απόφαση της ΕΕΤΤ ορίζεται η ημερομηνία απόσυρσης του αλγορίθμου. Εκτός κι αν ορίζεται διαφορετικά στην Απόφαση, κάθε ΠΥΕ υποχρεούται εντός έξι (6) μηνών από την ημερομηνία απόσυρσης του αλγορίθμου α) να ανακαλέσει όλα τα πιστοποιητικά των Αρχών Πιστοποίησης που χρησιμοποιούν αυτό τον αλγόριθμο β) να ανακαλέσει όλα τα τελικά πιστοποιητικά που χρησιμοποιούν αυτό τον αλγόριθμο και γ) να ενημερώσει κατάλληλα τους συνδρομητές του, εφόσον απαιτείται, ώστε να μην χρησιμοποιούν αυτό τον αλγόριθμο κατά τη υπογραφή ή σφράγιση εγγράφων. Οι εγκεκριμένοι ΠΥΕ υποχρεούνται να ενημερώνουν τον Εποπτικό Φορέα κατά την έναρξη και κατά την ολοκλήρωση της διαδικασίας. Μετά τη λήξη της ανωτέρω προθεσμίας, η ΕΕΤΤ προχωρά στην ενημέρωση του Καταλόγου Υπηρεσιών Εμπιστοσύνης, εφόσον απαιτείται.

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 ή 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 μετά την 1-6-2022. Εάν στο Κατάλογο Υπηρεσιών Εμπιστοσύνης περιλαμβάνεται η Αρχή Πιστοποίησης Ρίζας, προκειμένου να διατηρηθεί το καθεστώς της ως εγκεκριμένης υπηρεσίας, ο ΠΥΕ οφείλει να προσκομίσει στοιχεία που αποδεικνύουν ότι όλες οι υπηρεσίες που βασίζονται σε αυτήν δεν χρησιμοποιούν τον αλγόριθμο κατακερματισμού SHA-1. Κάθε ΠΥΕ υποχρεούται το αργότερο μέχρι την 1-6-2022 και ώρα 11:59:59πμ α) να ανακαλέσει όλα τα πιστοποιητικά των Υποκείμενων Αρχών Πιστοποίησης που χρησιμοποιούν τον αλγόριθμο SHA-1 και β) να ανακαλέσει όλα τα τελικά πιστοποιητικά που χρησιμοποιούν τον αλγόριθμο SHA-1.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

Άρθρο 14

Εποπτεία και Κυρώσεις

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

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.

Παράρτημα Α

Παραδείγματα επικύρωσης εγγράφου υπογεγραμμένου με SHA-1

Σκοπός του παραρτήματος είναι να διευκρινιστεί μέσω κατάλληλων παραδειγμάτων αν κατά την επικύρωση οι αλγόριθμοι του άρθρου 13 ισχύουν τη στιγμή της επικύρωσης ή τη στιγμή της εκτιμώμενης υπογραφής του εγγράφου.

Για το σκοπό αυτό εξετάζονται οι ακόλουθες περιπτώσεις:

α) αν την 1-7-2022 γίνει έλεγχος της εγκυρότητας μιας υπογραφής, που χρησιμοποιεί τον αλγόριθμο SHA-1, σε ένα έγγραφο που φέρει εγκεκριμένη χρονοσήμανση για την 1-7-2021, επίσης με SHA-1,

β) αν η υπογραφή της προηγούμενης περίπτωσης δεν φέρει εγκεκριμένη χρονοσήμανση αλλά χρονοσήμανση από την ημερομηνία/ώρα του υπολογιστή του υπογράφοντα και

γ) αν την 1-7-2022 γίνει έλεγχος της εγκυρότητας μιας υπογραφής, που χρησιμοποιεί τον αλγόριθμο SHA-1, σε ένα έγγραφο που φέρει εγκεκριμένη χρονοσήμανση για την 1-7-2021 επίσης με SHA-1, και νεότερη εγκεκριμένη χρονοσήμανση για την 1-8-2021 με SHA-256.

Καθώς οι περιορισμοί του άρθρου 13 για την ισχύ των αλγορίθμων δημιουργίας ζεύγους κλειδιών και των συναρτήσεων κατακερματισμού ελέγχονται τη στιγμή της επικύρωσης, το αποτέλεσμα της επικύρωσης των ανωτέρω εγγράφων, υποθέτοντας ότι η μόνη παράμετρος που την επηρεάζει είναι η εγκυρότητα ή μη της συνάρτησης κατακερματισμού SHA-1, θα είναι, ανά περίπτωση:

α) η υπογραφή είναι άκυρη καθώς, βάσει του άρθρου 13, παρ. 2, ο αλγόριθμος SHA-1 γίνεται δεκτός έως την 1-6-2022 ενώ η επικύρωση λαμβάνει χώρα την 1-7-2022, όταν ο αλγόριθμος πλέον θεωρείται μη αξιόπιστος,

β) η υπογραφή είναι άκυρη καθώς, βάσει του άρθρου 13, παρ. 2, ο αλγόριθμος SHA-1 γίνεται δεκτός έως την 1-6-2022 ενώ η επικύρωση λαμβάνει χώρα την 1-7-2022, όταν ο αλγόριθμος πλέον θεωρείται μη αξιόπιστος,, και

γ) η υπογραφή είναι έγκυρη με χρόνο υπογραφής του εγγράφου την 1-7-2021 καθώς την ημερομηνία εκείνη ο αλγόριθμος SHA-1 ήταν αποδεκτός και η νεότερη εγκεκριμένη χρονοσήμανση με SHA-256, που είναι ακόμα αξιόπιστος αλγόριθμος, τοποθετήθηκε πριν την 1-6-2022 και εξασφαλίζει την ακεραιότητα όλοι του εγγράφου, συμπεριλαμβανομένης της υπογραφής και της πρώτης χρονοσήμανσης με χρήση του αλγορίθμου SHA-1.

Διευκρινίζεται ότι σε όλες τις περιπτώσεις θεωρείται ότι τα εγκεκριμένα πιστοποιητικά δεν χρησιμοποιούν τον αλγόριθμο SHA-1. Επισημαίνεται ότι στις δύο πρώτες περιπτώσεις δεν εξαρτάται το αποτέλεσμα της ταυτοποίησης από τον αν έχει χρησιμοποιηθεί εγκεκριμένη χρονοσφραγίδα ή όχι, καθώς ακόμα και όταν αυτή υπάρχει, έχει τοποθετηθεί με χρήση SHA-1.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

ΠΡΟΤΕΙΝΟΜΕΝΟ ΠΕΡΙΕΧΟΜΕΝΟ

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

Άρθρο 1

Σκοπός και πεδίο εφαρμογής

Σκοπός της παρούσας είναι η ρύθμιση ειδικότερων ζητημάτων των υπηρεσιών εμπιστοσύνης και, συγκεκριμένα, θεμάτων που αφορούν στην ανάκληση εγκεκριμένων πιστοποιητικών. Από τις διατάξεις της παρούσας εξαιρούνται τα πιστοποιητικά μικρής διάρκειας (short-lived ή short-term certificates), όπως ορίζονται κατωτέρω, που δεν μπορούν να ανακληθούν (πρότυπο ETSI EN 319 411-1).

Για τους σκοπούς της παρούσας ισχύουν οι ορισμοί του άρθρου 3 του Κανονισμού (ΕΕ) 910/2014 (eIDAS) σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ και, επιπλέον οι διατάξεις του άρθρου 2 του ν.4727/2020.

Πιστοποιητικό μικρής διάρκειας: πιστοποιητικό με διάρκεια ισχύος (το χρονικό διάστημα μεταξύ της τιμής του πεδίου notBefore και αυτής του πεδίου notAfter συμπεριλαμβανομένης) μικρότερη από το μέγιστο χρόνο εντός του οποίου πρέπει να διεκπεραιωθεί ένα αίτημα ανάκλησης, δηλαδή 24 ώρες από την υποβολή του, σύμφωνα με το άρθρο 24, παρ. 3 του Κανονισμού (ΕΕ) 910/2014.

Άρθρο 2

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 319-411-2 σχετικά με τη συνάφεια της πληροφορίας που παρέχεται μέσω των δύο τρόπων ενημέρωσης. Η συμμόρφωση με την απαίτηση αυτή κατά την υλοποίηση του OCSP πρέπει να είναι τέτοια που να επιβάλλει τη χρήση της κατάστασης “unknown” ή “revoked” και να αποκλείει τη χρήση της κατάστασης “good”, στην περίπτωση υποβολής ερωτήματος για άγνωστο πιστοποιητικό, σύμφωνα με την ενότητα 2.2 του RFC6960.

Άρθρο 3

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

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

λήξη του πιστοποιητικού. Από την υποχρέωση αυτή εξαιρούνται τα πιστοποιητικά για την επαλήθευση της γνησιότητας ιστοτόπου.

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, όπου είναι τεχνικά εφικτό, να περιλαμβάνεται η επέκταση "archive cutoff" (RFC6960) με ημερομηνία αυτή της έναρξης του πιστοποιητικού της Αρχής Πιστοποίησης (Certificate Authority – CA, σύμφωνα με το πρότυπο ETSI EN 319 411-2) και να παρέχει πληροφόρηση για την κατάσταση κάθε πιστοποιητικού, ακόμα και μετά τη λήξη του.

   β. Αν το πιστοποιητικό μιας εκδότριας Αρχής Πιστοποίησης (CA) πρόκειται να λήξει τότε (i) αν ο ΠΥΕ δημοσιεύει CRL τότε μια τελική CRL πρέπει να εκδοθεί με ημερομηνία λήξης την 31 Δεκεμβρίου 9999, 23:59:59 ("99991231235959Z") και (ii) αν ο ΠΥΕ υλοποιεί μόνο OCSP, χωρίς να δημοσιεύει CRL, 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 ΠΥΕ τότε εφαρμόζονται οι προβλέψεις της ανωτέρω β΄ παραγράφου. Επιπλέον, ο ΠΥΕ πρέπει να διασφαλίζει ότι η τελική CRL ή/και οι τελικές απαντήσεις OCSP, όταν δεν δημοσιεύεται CRL, παραμένουν διαθέσιμες στα Βασιζόμενα Μέρη.

   δ. Ο ΠΥΕ ενημερώνει κατάλληλα τα συστήματά του για όλα τα πιστοποιητικά που έχουν λήξει ή ανακληθεί από όλες τις ενεργές εγκεκριμένες Αρχές Πιστοποίησης, ώστε να συμμορφώνονται με τα ανωτέρω, εντός τεσσάρων (4) μηνών από τη θέση σε ισχύ της παρούσας. Κάθε εγκεκριμένος ΠΥΕ υποχρεούται να ενημερώνει τον Εποπτικό Φορέα κατά την έναρξη της διαδικασίας ενημέρωσης των συστημάτων του, αναφέροντας κάθε τεχνικό περιορισμό που καθιστά αδύνατη την πλήρη συμμόρφωση, εφόσον υπάρχει, και κατά την ολοκλήρωσή της.

3. Σε κάθε περίπτωση, ο ΠΥΕ δημοσιεύει κατάλληλα στην Πολιτική Πιστοποίησης ή στη Δήλωση Πρακτικών Εμπιστοσύνης τον τρόπο συμμόρφωσης με τις απαιτήσεις του παρόντος άρθρου.

Καθηγ. Κωνσταντίνος Μασσέλος

ΠΡΟΕΔΡΟΣ ΕΕΤΤ

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr