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 34**

**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 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 45**

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

**Άρθρο 56**

**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. Δεν επιτρέπεται η χρήση ψευδώνυμων.

**Άρθρο 67**

**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 τεσσάρων (4) μηνών από τη δημοσίευσή της.

**Άρθρο 78**

**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 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.

**Με σχόλια [DZ1]:** Μετά από μια πολύ πρόσφατη εξέλιξη στο θέμα των ψευδωνύμων, σας παραθέτουμε δημόσια συζήτηση που πραγματοποιήθηκε στο CABF SMCWG στο οποίο συμμετέχει η GUnet/HARICA (https://lists.cabforum.org/pipermail/smcwg-public/2022-March/000291.html). Το mail thread αναφέρεται μεταξύ άλλων στο θέμα των ψευδωνύμων και από τη στιγμή που προβλέπεται από τον eIDAS, πρέπει να επιτρέπεται η δυνατότητα να υποστηριχθεί και από τους ΠΥΕ.

Σύμφωνα με τη συζήτηση, τα επικρατέστερα use cases αφορούν υπαλλήλους οργανισμών που δεν θέλουν να αποκαλυφθεί η πραγματική τους ταυτότητα. Γι' αυτό, στα πιστοποιητικά αυτά εμφανίζονται τα στοιχεία του Νομικού Προσώπου στο οποίο απασχολούνται ή συνεργάζονται, ο Πάροχος πραγματοποιεί ταυτοποίηση Φυσικού Προσώπου σύμφωνα με τα οριζόμενα στο Άρθρο 24-1, και στη θέση του ονοματεπώνυμου προσθέτει ένα ψευδώνυμο που αποτελείται από ένα τυχαίο αλλά μοναδικό αναγνωριστικό.
Η σύνδεση του ψευδώνυμου με το πραγματικό πρόσωπο μπορεί να γίνει μόνο από τον ΠΥΕ και μπορεί να δοθεί κατόπιν εισαγγελικής παραγγελίας ή απόδειξη έννομου συμφέροντος από κάποιον Τρίτο.

Με βάση τα παραπάνω, παρακαλούμε να επαναξιολογηθεί η επαναφορά της δυνατότητας χρήσης ψευδωνύμων υπό προϋποθέσεις που δεν θα επηρεάζουν αρνητικά τα Έμπιστα Μέρη.

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) για τα οποία υπάρχει δημόσια διαθέσιμη τεκμηρίωση στα Αγγλικά, Γαλλικά, Γερμανικά ή Ελληνικά που καθιστά δυνατό να διακριβωθεί χωρίς αμφισβήτηση ότι απαιτείται η φυσική παρουσία του φυσικού προσώπου για την έκδοση και την ανανέωσή τους και, τέλος,

   δ) εφόσον έχουν 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.

**Με σχόλια [DZ2]:** Δυστυχώς δεν μπορεί σήμερα να λειτουργήσει σε τεχνικό επίπεδο ο προτεινόμενος έλεγχος. Κάθε eIDAS Node φιλτράρει τους Identity Providers ως εξής:
- Notified or not
- Assurance level “Low, Substantial, High”

Δεν υπάρχει σήμερα τεχνικός τρόπος μέσω του eIDAS Node να αποκλειστεί ένας “Notified” κόμβος με επίπεδο διασφάλισης “Substantial” ή “High” με βάση πρόσθετα ειδικά κριτήρια του Service Provider (στη προκειμένη περίπτωση του ΠΥΕ).

Αν η ΕΕΤΤ θεωρεί ότι υπάρχουν “Notified” κόμβοι και Εθνικοί Identity Providers που **παραβιάζουν τον εκτελεστικό κανονισμό (ΕΕ) 2015/1502** -και ειδικότερα τα όσα αναφέρονται στην ενότητα 2.1.2- από συγκεκριμένα Κράτη Μέλη, καθώς η αρχική εγγραφή δεν γίνεται με φυσική παρουσία του φυσικού προσώπου, κατά τη γνώμη μας θα πρέπει να προχωρήσει σε συγκεκριμένη καταγγελία προς τις αρμόδιες αρχές του ΚΜ. Δεν είναι λογικό ο ΠΥΕ και ο κάθε Service Provider του σχήματος eID να ελέγχει διαρκώς τις περιοδικές εκθέσεις αναφοράς (peer reviews) των Κρατών Μελών προκειμένου να βασισθεί στις πληροφορίες αυτών, εφόσον η εποπτεία του eIDAS cooperation network έχει τους δικούς του ελεγκτικούς μηχανισμούς.

Επιπλέον, η διαδικασία της «Κοινοποίησης» αποτελεί διαδικασία Εθνικής δικαιοδοσίας με Εθνικές διασφαλίσεις που δεν μπορεί να τις αμφισβητήσει-απορρίψει ένας Service Provider του σχήματος (π.χ. ένας ΠΥΕ). Όλες οι αναφορές των Notified eID σχημάτων βρίσκονται δημοσιευμένες σε ιστοσελίδα της Ευρωπαϊκής Επιτροπής όπου η ΕΕΤΤ μπορεί να μελετήσει και να καταγγείλει πιθανές ασυνέπειες.

## 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, 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 γίνεται μετά την υποβολή της αίτησης τότε η αίτηση

μπορεί να υποβάλλεται με οποιοδήποτε τρόπο. Όταν χρησιμοποιείται το αποτέλεσμα προγενέστερης ταυτοποίησης τότε η αίτηση πρέπει να φέρει την ιδιόχειρη ή την εγκεκριμένη ηλεκτρονική υπογραφή του αιτούντα, οπότε και συστήνεται η χρήση εγκεκριμένης χρονοσφραγίδας, ή να γίνεται μέσω διαδικασίας που περιλαμβάνει την αποστολή μοναδικού κωδικού μιας χρήσης στο καταχωρισμένο κινητό του αιτούντα, ο οποίος απαιτείται να εισαχθεί από αυτόν στο πλαίσιο της διαδικασίας. 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 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 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 μπορεί να υποβάλλεται με απλή ηλεκτρονική υπογραφή του νόμιμου εκπροσώπου ή του ειδικά εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου. Όταν χρησιμοποιείται το αποτέλεσμα προγενέστερης ταυτοποίησης τότε 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 ή να γίνεται μέσω διαδικασίας που περιλαμβάνει την αποστολή μοναδικού κωδικού μιας χρήσης στο καταχωρισμένο κινητό του αιτούντα, ο οποίος απαιτείται να εισαχθεί από αυτόν στο πλαίσιο της διαδικασίας. 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 ιδιόχειρη ή εγκεκριμένη ηλεκτρονική υπογραφή 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.

**Άρθρο 10**

**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:

**Με σχόλια [DZ3]:** Η συγκεκριμένη παράγραφος αναφέρεται τόσο σε Πιστοποιητικά εγκεκριμένης όσο και σε προηγμένης ηλ. Υπογραφής. Αν κάποιος συνδρομητής έχει ήδη προηγμένη ηλ. Υπογραφή, είναι λογικό να μπορεί να την χρησιμοποιήσει για να την ανανεώσει. Προτείνεται να επιτρέπεται και η χρήση «προηγμένης ηλεκτρονικής υπογραφής του αιτούντα» στη διαδικασία της αίτησης:

*«Όταν χρησιμοποιείται το αποτέλεσμα προγενέστερης ταυτοποίησης τότε η αίτηση πρέπει να φέρει την ιδιόχειρη ή την εγκεκριμένη ή προηγμένη ηλεκτρονική υπογραφή του αιτούντα, οπότε και συστήνεται η χρήση εγκεκριμένης χρονοσφραγίδας»*

Σημειώνεται ότι και με την παραπάνω προτεινόμενη προσθήκη, η απαίτηση αυτή θα προκαλέσει δυσφορία και προβλήματα στους συνδρομητές καθώς η διαδικασία ηλ. υπογραφής στη φάση της αίτησης είναι «χειροκίνητη» διαδικασία (ο χρήστης θα πρέπει να κάνει download μια αίτηση σε PDF, να την υπογράψει και να την κάνει upload στον Πάροχο, ο οποίος θα πρέπει να την ελέγξει κλπ), απλά και μόνο για την αίτηση ανανέωσης. Σαν διαδικασία δεν μπορεί να κλιμακωθεί σε μεγάλους αριθμούς συνδρομητών που ζητούν επιτακτικά περισσότερη αυτοματοποίηση. Επισημαίνεται επίσης ότι σε κάθε περίπτωση έχει προηγηθεί ήδη η εξακρίβωση ταυτότητας με βάση το Άρθρο 24-1.

**Με σχόλια [DZ4]:** Η μέθοδος αποστολής OTP μέσω SMS εγκυμονεί σημαντικούς κινδύνους οι οποίοι αντιμετωπίζονται με έλεγχο δεύτερου παράγοντα είτε με TOTP είτε με WebAuthn (πρότυπο του W3C). Προτείνεται να μη γίνει τόσο συγκεκριμένη αναφορά σε αποστολή SMS αλλά να επιτραπούν και άλλες τεχνολογίες που είναι σαφώς πιο ασφαλείς. Προτείνεται η ακόλουθη αλλαγή:

*«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 κωδικών μιας χρήσης με χρονικό περιορισμό ή χρήση τεχνολογίας αντίστοιχης-καλύτερης διασφάλισης).»*

Το τελευταίο στοιχείο θα κάλυπτε την περίπτωση του WebAuthn.

**Με σχόλια [DZ5]:** Δεν είναι σαφής ο όρος «απλή ηλεκτρονική υπογραφή».

**Με σχόλια [DZ6]:** Αν η πρόθεση της ΕΕΤΤ είναι να υπάρχει αντίστοιχη διαδικασία με τις ηλ. Υπογραφές, προτείνεται να επιτρέπεται η χρήση «προηγμένης ή εγκεκριμένης ηλεκτρονικής υπογραφής του νόμιμου εκπροσώπου ή του ειδικά εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου ή την προηγμένη ηλ. Σφραγίδα του νομικού προσώπου».

Προτείνεται να γίνει:
*«η αίτηση πρέπει να φέρει την ιδιόχειρη ή εγκεκριμένη ή προηγμένη ηλεκτρονική υπογραφή του νόμιμου εκπροσώπου ή του ειδικά εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου ή την εγκεκριμένη ή προηγμένη ηλεκτρονική σφραγίδα του νομικού προσώπου».*

Σημειώνεται ότι σε κάθε περίπτωση έχει προηγηθεί ήδη η εξακρίβωση ταυτότητας με βάση το Άρθρο 24-1.

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. 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,

ii. 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, και

iii. 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 11**

**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 5 λεπτά της ώρας.
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 13, 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:

**Με σχόλια [DZ7]:** Δεν είναι σαφές το τι θεωρείται «εύλογο» στο επίπεδο διασφάλισης αυτής της απαίτησης. Προτείνεται να προστεθούν ενδεικτικά κάποια παραδείγματα που η ΕΕΤΤ θεωρεί εύλογα, όπως γίνεται και σε άλλα σημεία του κειμένου, ώστε κατ' ελάχιστον να μπορούν οι Πάροχοι και οι ΟΑΣ να θέτουν κάποια «όρια» παρ' όλη την ασάφεια.

**Με σχόλια [DZ8]:** Δεν είναι σαφές αν πρέπει να ικανοποιούνται ταυτόχρονα όλες οι εν λόγω απαιτήσεις ή όχι. Για παράδειγμα, όπως επισημάνθηκε στην προηγούμενη φάση της διαβούλευσης, η περίπτωση ii. δεν υποστηρίζεται από όλους τους κατασκευαστές ΕΔΔΥ οπότε αν είναι να ισχύουν ΚΑΙ ΟΙ ΤΡΕΙΣ προϋποθέσεις ταυτόχρονα, θα υπάρχει πρόβλημα στην εφαρμογή αυτής της διάταξης.

Πρακτικά, αν ισχύει το ii. (remote key attestation) με κρυπτογραφική επιβεβαίωση, επιβεβαιώνεται αυτόματα το i και iii. Αν δεν ισχύει το ii, ο ΠΥΕ πρέπει να λάβει τα μέτρα που προτείνονται στο i. και iii.

**Με σχόλια [DZ9]:** Το πρόβλημα αφορά κυρίως τα Relying Parties (RP). Από την απάντηση της ΕΕΤΤ φαίνεται ότι δεν έχει γίνει απολύτως κατανοητό το πρόβλημα οπότε επιτρέψτε μας να το αναλύσουμε λίγο καλύτερα.

Δεν τίθεται θέμα συγχρονισμού του ΠΥΕ με την ΣΠΩ. Αυτό ισχύει σε κάθε περίπτωση. Η ώρα notBefore στα πιστοποιητικά συνηθίζεται (ως καλή πρακτική) να τίθεται από τον Πάροχο **εσκεμμένα** κάποια (αρκετά) λεπτά νωρίτερα από την ΣΠΩ τη στιγμή έκδοσης του πιστοποιητικού προκειμένου να ξεπεραστεί το πρόβλημα συγχρονισμού. Για να γίνει πιο κατανοητό το πρόβλημα με το συγχρονισμό ρολογιών των RP, παραθέτουμε ένα χαρακτηριστικό παράδειγμα.

Ένας συνδρομητής που επείγεται να υπογράψει ένα κείμενο:
- Αποκτά ένα πιστοποιητικό με notBefore: 2022-03-08 13:21
- Υπογράφει ένα αρχείο ένα λεπτό αργότερα, στις 2022-03-08 13:22 με χρονοσήμανση την ώρα του υπολογιστή του υπογράφοντα.
- Στέλνει το έγγραφο σε ένα Relying Party στις 13:30 που έχει το ρολόι του υπολογιστή 1 ώρα πίσω (δηλαδή δείχνει 12:30).
- Το RP ξεκινά τη διαδικασία επικύρωσης της υπογραφής και διαπιστώνει ότι το πιστοποιητικό που χρησιμοποιήθηκε για την υπογραφή ΔΕΝ ΕΙΝΑΙ ΑΚΟΜΑ ΕΓΚΥΡΟ διότι δεν έχει φτάσει ακόμα ο χρόνος του notBefore (όσον αφορά τον υπολογιστή του RP).

Εκτιμούμε ότι 30 λεπτά είναι ένα πιο λογικό μέγιστο όριο απόκλισης από την πραγματική ώρα έκδοσης **του πιστοποιητικού** που καλύπτει λογικές αποκλίσεις ώρας των Έμπιστων Μερών για τα οποία -προφανώς- δεν μπορεί ο ΠΥΕ ή ο Συνδρομητής να έχει έλεγχο. Για αποκλίσεις πάνω από 30 λεπτά, είναι φυσιολογικό να εμφανιστούν και άλλα προβλήματα στα RP που θα πρέπει να βρουν τρόπο να το διορθώσουν μόνοι τους.

Επισημαίνεται ότι **η έναρξη ισχύος ενός πιστοποιητικού** κατά 30 λεπτά στο παρελθόν δεν δημιουργεί πρόβλημα ασφάλειας καθώς οι ηλεκτρονικές **υπογραφές** έχουν συνήθως χρονοσφραγίδα όπου φαίνεται η ημερομηνία/ώρα της πραγματικής υπογραφής.

Τέλος, το Παράρτημα Ι και ΙΙΙ του Κανονισμού στο σημείο ε) αναφέρει ότι το πιστοποιητικό πρέπει να έχει λεπτομέρειες για την έναρξη και τη λήξη της περιόδου ισχύος του Πιστοποιητικού χωρίς να προσδιορίζει αν πρέπει να μπει η στιγμή έκδοσης του πιστοποιητικού, ή η στιγμή που ολοκληρώθηκε η ταυτοποίηση του φυσικού προσώπου, ή κάτι άλλο.

**Με σχόλια [DZ10]:** Τεχνικά και πρακτικά, είναι αδύνατο να ελεγχθεί και να εφαρμοστεί αυτή η απαίτηση καθώς η εγκυρότητα/ακυρότητα μιας υπογραφής ελέγχεται αποκλειστικά από τα βασιζόμενα μέρη (Relying Parties). Ένα βασιζόμενο μέρος δεν μπορεί να έχει γνώση πότε παρέδωσε ένας ΠΥΕ ένα εγκεκριμένο πιστοποιητικό στον κάτοχό του για να εφαρμόσει αυτή την απαίτηση. Προτείνεται η αφαίρεση της παραγράφου.

α) Δεν επιτρέπεται η μεσολάβηση τρίτου για τη δημιουργία των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας, ή/και την εγκατάσταση του εγκεκριμένου πιστοποιητικού 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 8 ώρες την ημέρα και 5 ημέρες την εβδομάδα, 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 12**

**Διάρκεια ισχύος 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.
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 14 της παρούσας.

**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 (εγκεκριμένη χρονοσφραγίδα). Απουσία αξιόπιστης πηγής, η επικύρωση γίνεται στον τρέχοντα χρόνο.
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. 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

**Με σχόλια [DZ11]:** Δεν είναι κατανοητός ο λόγος αυτής της απαίτησης, δηλαδή ποιο πρόβλημα ασφάλειας προσπαθεί να λύσει/προλάβει. Το εγκεκριμένο πιστοποιητικό είναι Δημόσιο, συνεπώς αν υπάρχει βοήθεια τρίτου στην εγκατάσταση ενός Δημόσιου στοιχείου, δεν φαίνεται να υπάρχει κάποιο προφανές θέμα ασφάλειας.

Προφανώς δεν ισχύει το ίδιο με τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής/σφραγίδας που σωστά απαγορεύεται να γίνει με μεσολάβηση τρίτου.

Προτείνεται να αφαιρεθεί το δεύτερο μέρος της πρότασης.

**Με σχόλια [DZ12]:** Ένας Πάροχος μπορεί να μην έχει τη δυνατότητα λειτουργίας τηλεφωνικής υποστήριξης 8 ώρες την ημέρα και 5 ημέρες την εβδομάδα. Ειδικά σε περιόδους αργιών, μπορεί να υπάρχουν 4 ή 3 εργάσιμες σε μια εβδομάδα. Η συγκεκριμένη διατύπωση είναι προβληματική και δεν λαμβάνει υπ' όψιν αυτές τις περιπτώσεις. Σημειώνεται επίσης ότι για υποστήριξη 8 ωρών σημαίνει ότι απαιτούνται κατ' ελάχιστο **δύο εργαζόμενοι**, καθώς υπάρχει υποχρεωτικά ένα διάστημα προετοιμασίας της βάρδιας και ένα διάστημα κλεισίματος. Συνεπώς, το απολύτως ελάχιστο χρονικό διάστημα υποστήριξης δεν μπορεί να είναι 8 ώρες αλλά κάτω από 6 (αφήνοντας 1 ώρα προετοιμασία και 1 ώρα για το κλείσιμο στην 8ωρη εργασία, θεωρώντας ότι δεν υπάρχει διάλειμμα για τον εργαζόμενο εντός το 8ωρου).

Προτείνεται να αφαιρεθεί το συγκεκριμένο σημείο της πρότασης που αναφέρει *«τουλάχιστον για 8 ώρες την ημέρα και 5 ημέρες την εβδομάδα»*, και να υπάρχει γενικά η υποχρέωση παροχής δωρεάν τηλεφωνικής υποστήριξης εντός συγκεκριμένων εργάσιμων ωρών/ημερών που θα καθορίζει ο Πάροχος σε ιστοσελίδα του ή στο CP/CPS του.

**Με σχόλια [DZ13]:** Για να αποφευχθεί σύγχυση με τη χρήση του όρου «μπορεί» (φυσικά και «μπορεί» να ρυθμιστεί η λήξη ενός εγκεκριμένου πιστοποιητικού μετά τη λήξη της Αρχής Πιστοποίησης, αρκεί να το ρυθμίσει ένας Πάροχος), προτείνεται να αλλάξει σε *«πρέπει»* ώστε να αποτελεί παράβαση αν ο χρόνος notAfter του εγκεκριμένου πιστοποιητικού είναι μεγαλύτερος από το notAfter της ΑΠ έκδοσης.

**Με σχόλια [DZ14]:** Διαβάζοντας την αποδελτίωση του συγκεκριμένου σημείου, συμφωνούμε με την παρατήρηση της QMSCert διότι η χρονική στιγμή της υπογραφής είναι ουσιωδώς διαφορετική από τη χρονική στιγμή της επικύρωσης. Για παράδειγμα,

- Ένας συνδρομητής έχει ένα πιστοποιητικό εγκεκριμένης ηλεκτρονικής υπογραφής το οποίο λήγει στις 2020-03-10.
- Υπογράφει ηλεκτρονικά ένα έγγραφο στις 2020-03-08 14:13:03 και δεν προσθέτει εγκεκριμένη χρονοσφραγίδα αλλά την ημερομηνία/ώρα του υπολογιστή που έγινε η υπογραφή του εγγράφου.
- Κάποιο Έμπιστο Μέρος λαμβάνει το υπογεγραμμένο έγγραφο και ξεκινά τη διαδικασία επικύρωσης 2 χρόνια μετά, στις 2022-03-08 13:47:12.

Σύμφωνα με τη διατύπωση της παραγράφου 1. φαίνεται ότι κατά τη διαδικασία της επικύρωσης, η ημερομηνία/ώρα που πρέπει να χρησιμοποιηθεί **ως ημερομηνία/ώρα υπογραφής είναι η 20**[1]

**Με σχόλια [DZ15]:** Ειδικότερα με βάση την αποδελτίωση του συγκεκριμένου σημείου, προκύπτουν απαιτήσεις που η ΕΕΤΤ έχει υπ' όψιν (πχ ότι τα πιστοποιητικά εγκεκριμένων ηλ. Υπογραφών δεν θα πρέπει έχουν δημιουργηθεί με τον αλγόριθμο SHA-1) αλλά δεν εμφανίζονται στο σχέδιο της ΥΑ με αποτέλεσμα να μην είναι εφαρμόσιμες. Επίσης, χωρίς επιπλέον πληροφορίες, είναι πολύ πιθανό το συγκεκριμένο Άρθρο να υλοποιηθεί λανθασμένα από όσους θέλουν να κάνουν επικύρωση υπογραφής.

Η απάντηση της ΕΕΤΤ στο παράδειγμα της GUnet/HARICA για την περίπτωση γ) είναι πολύ χρήσιμη και αποδεικνύει ότι **οι συνθήκες του εγγράφου πριν τις 1-6-2022 μπορεί να καθορίσουν την μετέπειτα εγκυρότητα ή μη μιας ηλεκτρονικής υπογραφής που προστέθηκε με SHA-1 αλγόριθμο**. Κατά τη γνώμη μας είναι[2]

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. Στην περίπτωση που μια νέα έκδοση του προτύπου ETSI TS 119 312 καθιστά ένα αλγόριθμο μη αποδεκτό, κάθε ΠΥΕ υποχρεούται εντός τριών (3) μηνών από τη δημοσίευσή της α) να ανακαλέσει όλα τα πιστοποιητικά των Αρχών Πιστοποίησης που χρησιμοποιούν αυτό τον αλγόριθμο και β) να ανακαλέσει όλα τα τελικά πιστοποιητικά που χρησιμοποιούν αυτό τον αλγόριθμο. Οι εγκεκριμένοι ΠΥΕ υποχρεούνται να ενημερώνουν τον Εποπτικό Φορέα κατά την έναρξη και κατά την ολοκλήρωση της διαδικασίας.
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. Κάθε ΠΥΕ υποχρεούται το αργότερο μέχρι την 1-6-2022 και ώρα 11:59:59πμ α) να ανακαλέσει όλα τα πιστοποιητικά των Αρχών Πιστοποίησης που χρησιμοποιούν τον αλγόριθμο SHA-1 και β) να ανακαλέσει όλα τα τελικά πιστοποιητικά που χρησιμοποιούν τον αλγόριθμο SHA-1.

**Άρθρο 15**

**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.

**Με σχόλια [DZ16]:** Εκτιμούμε ότι 3 μήνες είναι πολύ μικρό διάστημα για ΟΛΙΚΟ rollover πιστοποιητικών/κλειδιών, ειδικά αν συζητάμε για πιστοποιητικά που χρησιμοποιούνται από σημαντικό μέρος του πληθυσμού της Χώρας αλλά και Συνδρομητές του εξωτερικού, συν τα Νομικά Πρόσωπα εντός και εκτός Χώρας. Εξαρτάται δε από το μέγεθος της αστοχίας ενός αλγορίθμου. Για παράδειγμα ο αλγόριθμος MD-5 είναι πλήρως παραβιάσιμος ενώ ο SHA-1 μερικώς.

Θυμίζουμε ότι ο αλγόριθμος SHA-1 είναι deprecated εδώ και πολλά χρόνια (από το 2005) και ακόμα χρησιμοποιείται.

Επιπλέον, επισημαίνουμε ότι χρειάζεται προσοχή με τις ανακλήσεις Αρχών Πιστοποίησης διότι ενδέχεται να προκαλέσει προβλήματα επικύρωσης υπογραφών ακόμα και στο διάστημα που υπήρχαν μη ανακλημένα εγκεκριμένα πιστοποιητικά, με αποτέλεσμα να ακυρωθούν όλες οι υπογραφές που είχαν προστεθεί στο παρελθόν για όλα τα πιστοποιητικά (ακόμα και όσα ήταν έγκυρα όταν είχαν υπογράψει έγγραφα). Χρειάζεται σημαντική διερεύνηση για τις πιθανές επιπτώσεις ανακλήσεων Αρχών Πιστοποίησης με βάση τα σημερινά πιο διαδεδομένα εργαλεία επικύρωσης υπογραφών (κυρίως Adobe Acrobat και DSS).

**Με σχόλια [DZ17]:** Τα Root CA πιστοποιητικά θα πρέπει να εξαιρούνται (βλ για παράδειγμα ένα σύντομο άρθρο: https://serverfault.com/questions/837994/why-are-ca-root-certificates-all-sha-1-signed-since-sha-1-is-deprecated).

Ο λόγος που επιτρέπεται μέχρι και σήμερα η εμπιστοσύνη σε SHA-1 πιστοποιητικά σε Root CAs τόσο στο WebPKI όσο και σε άλλες δημόσιες ιεραρχίες είναι ότι στο self-signed επίπεδο, δεν ελέγχεται η υπογραφή εντός του self-signed πιστοποιητικού αλλά μόνο το όνομα και το κλειδί (βλ. RFC 5280). Επίσης, ο SHA-1 αλγόριθμος είναι ευάλωτος σε collision attacks αλλά όχι σε pre-image attacks. Συνεπώς, σε ένα self-signed πιστοποιητικό, θεωρείται ότι όλες οι παράμετροι έχουν επιλεγεί από την CA και δεν υπάρχει πρακτικά τρόπος για να προκληθεί collision attack από κάποιον κακόβουλο. Ο μόνος τρόπος για να παραβιαστεί ένα SHA-1 self-signed πιστοποιητικό σήμερα είναι με παραγοντοποίηση RSA 2048 bit κλειδιού το οποίο είναι πρακτικά ανέφικτο.

Η HARICA περιλαμβάνει ένα ROOT CA self-signed πιστοποιητικό στην TSL (HaricaRootCA2011) με αλγόριθμο SHA-1 το οποίο είναι απόλυτα ασφαλές και θα θέλαμε να παραμείνει εντός της TSL μέχρι να λήξουν όλα τα τελικά πιστοποιητικά από τις ενεργές SHA-256 subCAs κάτω από τη συγκεκριμένη ιεραρχία.

## ΜΕΡΟΣ Β

## ΠΡΟΤΕΙΝΟΜΕΝΟ ΠΕΡΙΕΧΟΜΕΝΟ

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

**Άρθρο 8~~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 ν.4727/2020, αρ. …

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 9~~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 10~~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 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, 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.

**Με σχόλια [DZ18]:** Οι ρυθμίσεις για διατήρηση των ανακλημένων πιστοποιητικών μετά τη λήξη δεν πρέπει να αφορούν πιστοποιητικά γνησιότητας ιστοτόπων τα οποία είναι για authentication (άρα ο έλεγχος εγκυρότητας γίνεται την ώρα της αυθεντικοποίησης του ιστοτόπου) και πιθανότατα χρονοσφραγίδων ή συστημένης παράδοσης. Οι ρυθμίσεις διατήρησης κυρίως αφορούν πιστοποιητικά ηλ. Υπογραφών/Σφραγίδων.

Παρακαλούμε να διευκρινισθεί το εύρος εφαρμογής.

**Σελίδα 9: [1] Με σχόλια [DZ14]** **Dimitris Zacharopoulos** **9/3/2022 11:48:00 πμ**

Διαβάζοντας την αποδελτίωση του συγκεκριμένου σημείου, συμφωνούμε με την παρατήρηση της QMSCert διότι η χρονική στιγμή της υπογραφής είναι ουσιωδώς διαφορετική από τη χρονική στιγμή της επικύρωσης. Για παράδειγμα,

- Ένας συνδρομητής έχει ένα πιστοποιητικό εγκεκριμένης ηλεκτρονικής υπογραφής το οποίο λήγει στις 2020-03-10.
- Υπογράφει ηλεκτρονικά ένα έγγραφο στις 2020-03-08 14:13:03 και δεν προσθέτει εγκεκριμένη χρονοσφραγίδα αλλά την ημερομηνία/ώρα του υπολογιστή που έγινε η υπογραφή του εγγράφου.
- Κάποιο Έμπιστο Μέρος λαμβάνει το υπογεγραμμένο έγγραφο και ξεκινά τη διαδικασία επικύρωσης 2 χρόνια μετά, στις 2022-03-08 13:47:12.

Σύμφωνα με τη διατύπωση της παραγράφου 1. φαίνεται ότι κατά τη διαδικασία της επικύρωσης, η ημερομηνία/ώρα που πρέπει να χρησιμοποιηθεί **ως ημερομηνία/ώρα υπογραφής είναι η 2022-03-08 13:47:12**, το οποίο θα οδηγήσει στο συμπέρασμα ότι η υπογραφή είναι μη έγκυρη διότι το εγκεκριμένο πιστοποιητικό που χρησιμοποιήθηκε για την υπογραφή του εγγράφου **έληξε στις 2020-03-10**.

Αν αυτό είναι το επιθυμητό αποτέλεσμα που αναμένει η ΕΕΤΤ, παρακαλούμε να διευκρινιστεί λίγο καλύτερα, ίσως με την ακόλουθη διατύπωση:

*«Απουσία αξιόπιστης πηγής, ως χρόνος υπογραφής του εγγράφου θα χρησιμοποιείται η τρέχουσα ημερομηνία/ώρα που θα συμπίπτει με τη χρονική στιγμή της επικύρωσης»*.

Για λόγους καλύτερης κατανόησης, αναφέρουμε ότι η επικύρωση μιας υπογραφής γίνεται ΠΑΝΤΑ στον εκάστοτε τρέχοντα χρόνο. Επικύρωση μιας υπογραφής μπορεί να γίνει σε άπειρες χρονικές στιγμές, ακόμα και 10 χρόνια μετά την εισαγωγή της υπογραφής.

**Σελίδα 9: [2] Με σχόλια [DZ15]** **Dimitris Zacharopoulos** **9/3/2022 11:51:00 πμ**

Ειδικότερα με βάση την αποδελτίωση του συγκεκριμένου σημείου, προκύπτουν απαιτήσεις που η ΕΕΤΤ έχει υπ' όψιν (πχ ότι τα πιστοποιητικά εγκεκριμένων ηλ. Υπογραφών δεν θα πρέπει έχουν δημιουργηθεί με τον αλγόριθμο SHA-1) αλλά δεν εμφανίζονται στο σχέδιο της ΥΑ με αποτέλεσμα να μην είναι εφαρμόσιμες. Επίσης, χωρίς επιπλέον πληροφορίες, είναι πολύ πιθανό το συγκεκριμένο Άρθρο να υλοποιηθεί λανθασμένα από όσους θέλουν να κάνουν επικύρωση υπογραφής.

Η απάντηση της ΕΕΤΤ στο παράδειγμα της GUnet/HARICA για την περίπτωση γ) είναι πολύ χρήσιμη και αποδεικνύει ότι **οι συνθήκες του εγγράφου πριν τις 1-6-2022 μπορεί να καθορίσουν την μετέπειτα εγκυρότητα ή μη μιας ηλεκτρονικής υπογραφής που προστέθηκε με SHA-1 αλγόριθμο**. Κατά τη γνώμη μας είναι σημαντικό να διευκρινιστούν-προστεθούν τα ακόλουθα στο σχέδιο της ΥΑ:

- Αν ένα έγγραφο υπογραφεί με εγκεκριμένο πιστοποιητικό που έχει εκδοθεί με χρήση του αλγορίθμου SHA-1, ανεξαρτήτως του αλγορίθμου υπογραφής του εγγράφου, η επικύρωση μετά την 1-6-2022 θα εμφανίζει την υπογραφή άκυρη.
- Αν ένα έγγραφο υπογραφεί με ένα εγκεκριμένο πιστοποιητικό που εκδόθηκε με χρήση αλγόριθμου που θεωρείται ασφαλής με βάση το Άρθρο 14 της παρούσας (δηλαδή όχι SHA-1), και η υπογραφή του εγγράφου χρησιμοποιεί αλγόριθμο SHA-1 χωρίς κάποια συμπληρωματική υπογραφή με ασφαλή αλγόριθμο που εξασφαλίζει την ακεραιότητα του αρχικού εγγράφου, η επικύρωση μετά την 1-6-2022 θα εμφανίζει την υπογραφή άκυρη.

- Αν ένα έγγραφο υπογραφεί με ένα εγκεκριμένο πιστοποιητικό που εκδόθηκε με χρήση αλγόριθμου που θεωρείται ασφαλής με βάση το Άρθρο 14 της παρούσας (δηλαδή όχι SHA-1), η υπογραφή του εγγράφου χρησιμοποιεί αλγόριθμο SHA-1 και υπάρχει κάποια συμπληρωματική υπογραφή με ασφαλή αλγόριθμο που εξασφαλίζει την ακεραιότητα του αρχικού εγγράφου και προστεθεί πριν την 1-6-2022, τότε η επικύρωση μετά την 1-6-2022 θα εμφανίζει την υπογραφή έγκυρη.