Αποτελέσματα Δημόσιας Διαβούλευσης

Σχόλια συμμετεχόντων και θέση της ΕΕΤΤ

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

Επί του προτεινόμενου κειμένου της Υπουργικής Απόφασης που προβλέπεται στο αρ. 107, παρ. 31 του Ν.4727/2020

Άρθρο 3

Δύο συμμετέχοντες (GUnet, QMSCert) σχολίασαν ότι θα πρέπει να αποσαφηνιστεί κατά πόσον η συμμόρφωση με τις συστάσεις που δημοσιεύει ο ENISA είναι υποχρεωτική και ότι οι συστάσεις/ μελέτες του ENISA δεν έχουν κανονιστικό αλλά συμβουλευτικό χαρακτήρα και η προτεινόμενη γενική αναφορά στα κείμενα του ENISA δεν είναι εύκολα εφαρμόσιμη και θα έχει σημαντικές συνέπειες στο κόστος και στο χρόνο επιθεώρησης και έκδοσης της ΕΑΣ. Η ΕΕΤΤ κάνει δεκτό το σχόλιο και διαγράφει το άρθρο.

Άρθρο 4, παρ. 1

1. Ένας συμμετέχοντας (Byte) σχολίασε ότι ο αριθμός φορολογικού μητρώου του ΠΥΕ, πρέπει να δηλώνεται ως "VATEL" στο χαρακτηριστικό "organizationIdentifier" του πεδίου Εκδότης ενώ αν απαιτείται άλλη τιμή εκτός του ΑΦΜ τότε αυτή πρέπει να δηλώνεται στο χαρακτηριστικό "OU". Στις υπάρχουσες Αρχές Πιστοποίησης δε, προτείνει τη χρήση του χαρακτηριστικού "OU" ως εξής: "OU = Issued by … VATEL-…". Τρεις συμμετέχοντες (Byte, GUnet και QMSCert) σχολίασαν ότι η φράση «Ο κωδικός χώρας σε όλες τις άλλες περιπτώσεις είναι "EL"» είναι αντίθετη με το πρότυπο, που προβλέπει τον κωδικό ISO 3166-1 της χώρας, που είναι "GR", αλλά και ασαφής καθώς δεν προσδιορίζονται οι «άλλες περιπτώσεις». Η ΕΕΤΤ αναγνωρίζει ότι η συγκεκριμένη παράγραφος χρειάζεται να διατυπωθεί έτσι ώστε να ορίζονται τόσο το πεδίο, όσο και το χαρακτηριστικό στο οποίο δηλώνεται αλλά και η μορφή που πρέπει να έχει η δήλωση του αριθμού μητρώου του εγκεκριμένου ΠΥΕ στα εγκεκριμένα πιστοποιητικά. Επιπλέον, κάνει δεκτό το σχόλιο αναφορικά με τη φράση «Ο κωδικός χώρας σε όλες τις άλλες περιπτώσεις είναι "EL"» ενώ κρίνει σκόπιμο να διευκρινίζεται η προτίμηση στη χρήση του κωδικού χώρας "EL" για τα προθέματα "TIN" και "VAT". Αναφορικά με τη χρήση του χαρακτηριστικού "OU", η ΕΕΤΤ κρίνει ότι δεν απαιτείται να οριστεί επακριβώς το πεδίο και η μορφή που πρέπει να έχει η δήλωση στην περίπτωση ήδη εγκεκριμένων Αρχών Πιστοποίησης, που δεν περιλαμβάνουν τον αριθμό μητρώου του εγκεκριμένου ΠΥΕ στο πεδίο Υποκείμενο του πιστοποιητικού τους. Τέλος, κρίνεται σκόπιμο να οριστεί η υποχρέωση ανάκλησης όλων των εγκεκριμένων πιστοποιητικών που έχουν εκδοθεί κατά τη θέση σε ισχύ της παρούσας και δεν ικανοποιούν την ανωτέρω απαίτηση εντός ευλόγου χρονικού διαστήματος. Επιπλέον,

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

για λόγους σαφήνειας του κειμένου, κρίνεται σκόπιμο να μεταφερθεί το περιεχόμενο που αφορά στις ήδη εγκεκριμένες Αρχές Πιστοποίησης και στην υποχρέωση ανάκλησης σε 2 ξεχωριστές παραγράφους.

Άρθρο 4, παρ. 2

1. Ένας συμμετέχοντας (GUnet) σχολίασε ότι, εφόσον χρησιμοποιηθεί η επιλογή <RT:EL-αριθμός καταχώρισης στο αρχείο της ΕΕΤΤ>, τότε ισχύει η τελευταία παράγραφος της ενότητα 5.1.4 του προτύπου ETSI EN 319 412-1, που 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 generalName. The two letter identity type reference following the ":" character shall be unique within the context of the specified uniformResourceIdentifier". Η ΕΕΤΤ κάνει δεκτό το σχόλιο και τροποποιεί την παράγραφο κατάλληλα.

2. Ένας συμμετέχοντας (Adacom) σχολίασε ότι εφόσον χρειάζεται να συμπεριλαμβάνεται ο αριθμός καταχώρισης του εγκεκριμένου ΠΥΕ στο αρχείο της ΕΕΤΤ ή οποιοδήποτε άλλο στοιχείο, αυτά μπορούν να δηλώνονται στο χαρακτηριστικό "OU". Η ΕΕΤΤ διευκρινίζει ότι η συγκεκριμένη παράγραφος αναφέρεται στο χαρακτηριστικό "organizationIdentifier" και προσφέρει μια εναλλακτική επιλογή χρήσης του αριθμού καταχώρισης στο αρχείο της ΕΕΤΤ αντί του ΑΦΜ ή του αρ. ΓΕΜΗ κι αυτό σε ειδικές περιπτώσεις. Κατά συνέπεια, η ΕΕΤΤ κρίνει ότι δεν χρειάζεται να τροποποιηθεί το άρθρο και απορρίπτει το συγκεκριμένο σχόλιο.

Άρθρο 4, παρ. 4

1. Ένας συμμετέχοντας (Adacom) πρότεινε να αναφερθεί σαφώς ότι ο αριθμός μητρώου πρέπει να δηλώνεται σύμφωνα με τα οριζόμενα προηγουμένως και να αυξηθεί το χρονικό διάστημα συμμόρφωσης από τον 1 στους 6 μήνες. Η ΕΕΤΤ κάνει δεκτό το σχόλιο στο πρώτο σκέλος και απορρίπτει το δεύτερο, τροποποιώντας την παράγραφο κατάλληλα.

Άρθρο 5

1. Ένας συμμετέχοντας (GUnet) σχολίασε ότι ο τίτλος του άρθρου είναι λάθος καθώς το σωστό είναι Παράρτημα III και όχι Παράρτημα II του Κανονισμού eIDAS. Πρότεινε δε να αλλαχτεί σε «Παράρτημα III, σημείο γ» ώστε να είναι πιο πλήρες. Η ΕΕΤΤ κάνει δεκτό το σχόλιο.

2. Όλοι οι συμμετέχοντες σχολίασαν τη φράση «Ο κωδικός χώρας σε όλες τις άλλες περιπτώσεις είναι "EL"» παραπέμποντας στα σχόλιά τους στο άρθρο 4. Η ΕΕΤΤ κάνει δεκτό το σχόλιο και τροποποιεί το άρθρο κατάλληλα.

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

3. Ένας συμμετέχοντας (QMSCert) πρότεινε να εισαχθεί ξεχωριστή παράγραφος σχετικά με το σωστό χειρισμό των κωδικών χώρας "EL" και "GR". Η ΕΕΤΤ θεωρεί ότι το κείμενο των άρθρων 4 και 5, όπως προέκυψε μετά τις τροποποιήσεις, είναι σαφές και δεν χρειάζεται να μεταφερθεί το κείμενο για το χειρισμό των "EL" και "GR" σε ξεχωριστή παράγραφο.

Άρθρο 6

1. Δύο συμμετέχοντες (Byte, GUnet) εκφράζουν αμφιβολίες σχετικά με τη χρήση ψευδωνύμων λόγω έλλειψης διεθνώς αποδεκτών κριτηρίων επαλήθευσής τους και προτείνουν είτε την απαγόρευσή τους είτε την εισαγωγή κριτηρίων. Η ΕΕΤΤ διευκρινίζει ότι στόχος της πρόβλεψης είναι να οριστεί ο τρόπος με τον οποίο δηλώνονται ψευδώνυμα στα τελικά πιστοποιητικά. Η συμμόρφωση των κριτηρίων με βάση τα οποία αυτά εισάγονται ελέγχεται άλλωστε από Οργανισμό Αξιολόγησης Συμμόρφωσης για τα εγκεκριμένα πιστοποιητικά. Για λόγους σαφήνειας και μόνο, η ΕΕΤΤ αποφασίζει να περιλάβει σχετική διάταξη στην πρότασή της. Ένας άλλος συμμετέχοντας (GUnet) σχολίασε ότι ενδέχεται να υπάρχουν περιπτώσεις οργανισμών ή δημόσιων υπηρεσιών (π.χ. ΕΥΠ) που δεν επιθυμούν στα τελικά πιστοποιητικά των υπαλλήλων τους να περιλαμβάνεται το ονοματεπώνυμό τους για λόγους ασφάλειας αλλά μόνο κάποιο κατάλληλο ψευδώνυμο. Η ΕΕΤΤ επισημαίνει ότι δεν έλαβε σχετικό αίτημα από κανένα οργανισμό κατά τη διάρκεια της δημόσιας διαβούλευσης που να τεκμηριώνει την ανάγκη για μια τέτοια πρόβλεψη. Επιπλέον, λαμβάνοντας υπόψη την υποχρέωση των παρόχων να δίνουν τα στοιχεία του φυσικού ή νομικού προσώπου που είναι κάτοχος ενός πιστοποιητικού, όταν τα ζητά κάποιο έμπιστο μέρος, η ΕΕΤΤ θεωρεί ότι κατάλληλο να ορίσει εξαιρέσεις σε αυτή την υποχρέωση όταν χρησιμοποιούνται ψευδώνυμα, είναι το Υπουργείο.

2. Ένας συμμετέχοντας (QMSCert) ζητά να διευκρινιστεί ότι η λέξη "PSEUDONYM" περιλαμβάνεται στο στοιχείο commonName μόνο όταν χρησιμοποιείται ψευδώνυμο. Η ΕΕΤΤ επισημαίνει ότι η πρόβλεψη αυτή αφορά μόνο στην περίπτωση που στο τελικό πιστοποιητικό περιλαμβάνεται ψευδώνυμο, οπότε δηλώνεται τόσο στο στοιχείο pseudonym όσο και στο commonName σύμφωνα με τα οριζόμενα σ' αυτήν, είναι δε σαφής και δεν χρειάζεται περαιτέρω διευκρίνιση.

3. Σύμφωνα με το ETSI EN 319 412-2, δεν επιτρέπεται η ταυτόχρονη συμπερίληψη ψευδωνύμου και ονοματεπώνυμου στο τελικό πιστοποιητικό. Η ΕΕΤΤ εισάγει διάταξη που να καθιστά την πρόβλεψη αυτή του προτύπου υποχρεωτική.

Άρθρο 7

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

1. Η ΕΕΤΤ διαπιστώνει ότι δεν περιλαμβάνεται πρόβλεψη για το περιεχόμενο των πιστοποιητικών επαλήθευσης της γνησιότητας ιστοτόπου. Κατά συνέπεια, στο άρθρο προστίθεται νέα παράγραφος με κατάλληλο περιεχόμενο.

2. Η ΕΕΤΤ κρίνει ότι πρέπει να οριστεί διάστημα συμμόρφωσης των ΠΥΕ με τα οριζόμενα στις τρεις πρώτες παραγράφους του άρθρου. Κατά συνέπεια, προστίθεται τέταρτη παράγραφος με προτεινόμενο διάστημα συμμόρφωσης τους 6 μήνες.

Άρθρο 8

1. Ένας συμμετέχοντας (QMSCert) σχολίασε ότι η πρώτη παράγραφος πρέπει να τροποποιηθεί ώστε να είναι ξεκάθαρο ότι η ταυτοποίηση πρέπει να έχει διενεργηθεί πριν την έκδοση του πιστοποιητικού και το χρονικό διάστημα μεταξύ αυτής και της έκδοσης δεν μπορεί να είναι μεγαλύτερο του ενός έτους. Η ΕΕΤΤ κάνει εν μέρει δεκτό το σχόλιο και τροποποιεί την παράγραφο κατάλληλα.

2. Τρεις συμμετέχοντες (Adacom, AthEx, Byte) σχολίασαν ότι καθώς όλες οι μέθοδοι είναι ισοδύναμες, θα πρέπει η ισχύς του αποτελέσματος της ταυτοποίησης να είναι για όλες 1 έτος. Ένας συμμετέχοντας (GUnet) σχολίασε ότι η μέθοδος του άρθρου 24, παρ. 1, σημείο δ) του Κανονισμού eIDAS είναι ισοδύναμη με αυτή του σημείου α) και, κατά συνέπεια, θα πρέπει η ισχύς του αποτελέσματος της ταυτοποίησης με τη μέθοδο αυτή να είναι 1 έτος. Η ΕΕΤΤ αποδέχεται το σχόλιο που αφορά στη μέθοδο του άρθρου 24, παρ. 1, σημείο δ), καθώς είναι ισοδύναμη της φυσικής παρουσίας, αλλά απορρίπτει το αίτημα που αφορά στις μεθόδους των σημείων β) και γ), καθώς οι μέθοδοι αυτές είναι απλές χωρίς να απαιτούν κάποια ιδιαίτερη ενέργεια από τον αιτούντα.

3. Για τη διευκόλυνση των πολιτών, κρίνεται σκόπιμη η προσθήκη πρόβλεψης για τη δυνατότητα επιβεβαίωσης της ταυτοποίησης με φυσική παρουσία μέσω της βεβαίωσης του γνησίου της υπογραφής του αιτούντα στην αίτηση έκδοσης εγκεκριμένου πιστοποιητικού από αρμόδια Διοικητική Αρχή ή ΚΕΠ με αυτοπρόσωπη παρουσία του υπογράφοντα. Στο πλαίσιο αυτό, είναι απαραίτητο να διευκρινιστεί ότι η χρήση της εφαρμογής «Ψηφιακή Βεβαίωση Εγγράφου» από την πλατφόρμα gov.gr δεν πληροί τις απαιτήσεις του άρθρου 24, παρ. 1, σημείο α του Κανονισμού eIDAS.

4. Δύο συμμετέχοντες (Adacom, Byte) σχολίασαν ότι η απαίτηση του σημείου β) της 3ης παραγράφου είναι υπερβολική καθώς δεν επιβάλλεται από τον Κανονισμό eIDAS, φέρνει τους εγχώριους παρόχους σε μειονεκτική θέση έναντι των ανταγωνιστών τους στο εξωτερικό, οι οποίοι δεν έχουν τέτοια

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

υποχρέωση, μπορεί να εφαρμοστεί μόνο σε εγχώριους παρόχους και, τέλος, αυξάνει σημαντικά τα λειτουργικά κόστη. Η ΕΕΤΤ αρχικά επισημαίνει ότι η σχετική απαίτηση επιβάλλεται από τον Κανονισμό eIDAS, ο οποίος στο άρθρο 24, παρ. 1, σημείο γ) αναφέρει σαφώς «μέσω πιστοποιητικού εγκεκριμένης ηλεκτρονικής υπογραφής ή εγκεκριμένης ηλεκτρονικής σφραγίδας που έχει εκδοθεί σύμφωνα με το στοιχείο α) ή β),». Κατά συνέπεια, η ΕΕΤΤ θεωρεί ότι η παράγραφος αυτή επιβάλλει πρόσθετη υποχρέωση τήρησης στοιχείων στο αρχείο του παρόχου και μόνο, οι δε ισχυρισμοί περί μειονεκτικής θέσης των εγχώριων παρόχων έναντι των ανταγωνιστών τους στο εξωτερικό είναι αβάσιμοι καθώς ο Κανονισμός eIDAS ισχύει σε όλα τα Κράτη Μέλη. Επομένως, η ΕΕΤΤ απορρίπτει τα σχόλια των παρόχων κρίνοντας ότι δεν απαιτείται τροποποίηση του συγκεκριμένου σημείου.

5. Ένας συμμετέχοντας (QMSCert) σχολίασε ότι στο σημείο β) της 3ης παραγράφου γίνεται ένα νομικό άλμα καθώς επεκτείνεται η πρόβλεψη του άρθρου 24, παρ. 1, σημείο γ) του Κανονισμού eIDAS και σε εγκεκριμένα πιστοποιητικά που έχουν εκδοθεί με τη μέθοδο του άρθρου 24, παρ. 1, σημείο δ), για το οποίο απαιτείται τεκμηρίωση. Η ΕΕΤ διευκρινίζει κατ' αρχάς ότι το άρθρο 24, παρ. 1, σημείο γ) δεν επιτρέπει την έκδοση ενός νέου εγκεκριμένου πιστοποιητικού βάσει ενός ισχύοντος εγκεκριμένου πιστοποιητικού που έχει εκδοθεί με την ίδια μέθοδο. Πέραν αυτού, όπως προβλέπει το σημείο δ) του ίδιου άρθρου, εθνική νομοθεσία μπορεί να ορίσει άλλες μεθόδους ταυτοποίησης ως ισοδύναμες της φυσικής παρουσίας. Κατά συνέπεια, κάθε εγκεκριμένο πιστοποιητικό που εκδίδεται μέσω κάποιας από τις μεθόδους ταυτοποίησης του σημείου δ), μπορεί να θεωρηθεί ότι εκδίδεται με τη μέθοδο του σημείου α) (φυσική παρουσία) και, επομένως, πληρείται η απαίτηση της μεθόδου του σημείου γ) και για τις μεθόδους αυτές. Η ΕΕΤΤ κρίνει ότι δεν απαιτείται περαιτέρω τεκμηρίωση για το σημείο αυτό, έχει δε προστεθεί απλά για λόγους πληρότητας και σαφήνειας.

6. Τρεις συμμετέχοντες (Byte, GUnet, QMSCert) εξέφρασαν την αντίρρησή τους σχετικά με την πρόβλεψη της 4ης παραγράφου. Θεωρούν την απαίτηση άδικη καθώς δεν ισχύει για άλλα Κράτη Μέλη δημιουργώντας πρόβλημα με τον ανταγωνισμό καθώς και ότι οι 3 μέρες ενδεχομένως να μην επαρκούν ιδίως σε περιόδους αργιών, διακοπών κ.λπ. Επιπλέον, εκφράζονται φόβοι για κατάχρηση της δυνατότητας αυτής από κάποιο πάροχο προκειμένου να προκαλέσει αυξημένο φόρτο εργασίας στους ανταγωνιστές του, αμφιβολίες σχετικά με τον τρόπο που υποβάλλεται ένα τέτοιο αίτημα αλλά και ανησυχία για ενδεχόμενη άρνηση παροχής στοιχείων και προτείνεται είτε η υλοποίηση κάποιας πλατφόρμας από την ΕΕΤΤ είτε τον ορισμό της μεθόδου με λεπτομέρεια ώστε να είναι

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

αυτοματοποιημένη. Η ΕΕΤΤ σημειώνει ότι σκοπός αυτής της παραγράφου είναι να διασφαλίσει ότι θα καταστεί δυνατή η χρήση της μεθόδου ταυτοποίησης του άρθρου 24, παρ. 1, σημείο γ) και για εγκεκριμένα πιστοποιητικά που έχουν εκδοθεί από άλλο πάροχο. Ο ισχυρισμός ότι αντίστοιχη υποχρέωση δεν υπάρχει σε άλλα Κράτη Μέλη δεν είναι ορθός καθώς, για παράδειγμα, στην Ισπανία το άρθρο 7, παρ. 3 του ν.6/2020 αναφέρει ότι «Η μέθοδος μέσω της οποίας ταυτοποιήθηκε ο αιτών το εγκεκριμένο πιστοποιητικό, μπορεί να εμφανίζεται στο πιστοποιητικό. Αλλιώς, οι πάροχοι υπηρεσιών εμπιστοσύνης οφείλουν να συνεργάζονται μεταξύ τους προκειμένου να διαπιστωθεί η τελευταία φορά που ο αιτών ταυτοποιήθηκε με φυσική παρουσία». Η ΕΕΤΤ αποδέχεται την παρατήρηση σχετικά με την ασάφεια της προθεσμίας των 3 ημερών αλλά και ότι είναι υπερβολικά αυστηρή. Αναφορικά με τη διαδικασία υποβολής του αιτήματος, η θέση της ΕΕΤΤ είναι ότι η δημιουργία πλατφόρμας για τη διεκπεραίωση τέτοιων αιτημάτων είναι μάλλον υπερβολική. Αναγνωρίζει όμως το βάσιμο του προβληματισμού που εκφράστηκε σχετικά με την υποβολή μεγάλου αριθμού αιτημάτων από κάποιο πάροχο στους ανταγωνιστές του. Βάσει των ανωτέρω, η ΕΕΤΤ τροποποιεί τη συγκεκριμένη παράγραφο κατάλληλα.

7. Η ΕΕΤΤ διαπιστώνει ότι υπάρχει κενό σχετικά με την εφαρμογή της μεθόδου ταυτοποίησης του άρθρου 24, παρ. 1, σημείο γ) του Κανονισμού eIDAS. Κατά συνέπεια, προστίθεται νέα παράγραφος αμέσως μετά την παράγραφο 2 με τις υποχρεώσεις που ισχύουν σωρευτικά για τον πάροχο.

Άρθρο 9

1. Τρεις συμμετέχοντες (Byte, GUnet, QMSCert) σχολίασαν την απαίτηση ύπαρξης ιδιόχειρης ή εγκεκριμένης υπογραφής στην αίτηση του αιτούντα, προτείνοντας τη χρήση άλλων τρόπων και αναφέροντας ότι η απαίτηση δεν είναι εφαρμόσιμη στις περιπτώσεις ταυτοποίησης με τις μεθόδους του άρθρου 24, παρ. β και δ του Κανονισμού eIDAS. Η ΕΕΤΤ αποδέχεται το σχόλιο, επισημαίνοντας όμως ότι πρέπει να τεθεί μία διάκριση ως προς τη διασφάλιση που απαιτείται όταν η αίτηση γίνεται πριν ή μετά την ταυτοποίηση. Κι αυτό γιατί αν έχει προηγηθεί η ταυτοποίηση, τότε πρέπει να υπάρχει μεγαλύτερο επίπεδο διασφάλισης της εγκυρότητας της αίτησης από ότι όταν η ταυτοποίηση γίνεται σε επόμενο στάδιο. Επιπλέον, η χρήση πιο απλών μεθόδων υπογραφής της αίτησης, συνεπάγεται ορισμένες πρόσθετες υποχρεώσεις για τους εγκεκριμένους ΠΥΕ. Στο πλαίσιο αυτό, κρίνεται ότι η απαίτηση ύπαρξης ιδιόχειρης υπογραφής δεν επαρκεί και πρέπει να βεβαιώνεται το γνήσιο αυτής στην αίτηση από κατάλληλη Αρχή. Τέλος, η ΕΕΤΤ κρίνει ότι άλλες

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

μέθοδοι, που περιλαμβάνουν π.χ. την αποστολή κωδικού μιας χρήσης στο κινητό του αιτούντα είναι εξίσου ασφαλείς.

2. Δύο συμμετέχοντες (Adacom, Byte) προτείνουν την επέκταση της διάρκειας ισχύος της αίτησης από τους 3 στους 12 μήνες. Η πρόταση απορρίπτεται καθώς η αίτηση αφορά αποκλειστικά και μόνο στην έκδοση ενός εγκεκριμένου πιστοποιητικού, οπότε και παύει να έχει κάποια ισχύ όταν αυτό εκδοθεί, και κανείς από τους δύο που υπέβαλαν σχόλια δεν αναφέρει κάποιο λόγο για τον οποίο κάποιος θα υπέβαλε αίτηση κάποια στιγμή και θα λάμβανε το εγκεκριμένο πιστοποιητικό που αιτήθηκε 1 χρόνο αργότερα.

3. Ένας συμμετέχοντας (QMSCert) πρότεινε να διευκρινιστεί αν επιτρέπεται η υποβολή αίτησης από εξουσιοδοτημένο ή πληρεξούσιο πρόσωπο. Η ΕΕΤΤ κρίνει ότι δεν θεωρείται σκόπιμη η προσθήκη ειδικών διατάξεων που ρυθμίζουν θέματα πληρεξουσιότητας.

4. Βάσει των ανωτέρω, το άρθρο 9 τροποποιείται κατάλληλα.

Άρθρο 10

1. Δύο συμμετέχοντες (GUnet, QMSCert) σχολίασαν ότι το άρθρο 26, παρ. γ του Κανονισμού eIDAS απαιτεί τη διασφάλιση της αποκλειστικής χρήσης του κλειδιού από το συνδρομητή, δηλαδή αποκλειστικής δυνατότητας υπογραφής, και όχι δημιουργίας του ζεύγους κλειδιών. Η ΕΕΤΤ επιβεβαιώνει ότι σκοπός της πρώτης παραγράφου του άρθρου αυτού είναι να επιβάλει τη σχετική υποχρέωση στον πάροχο να επιβεβαιώνει ότι ο συνδρομητής έχει τη δυνατότητα να χρησιμοποιεί σωστά την ΕΔΔΥ και αναγνωρίζει τη χρήση της λάθος λέξης «δημιουργεί» αντί της σωστής «χρησιμοποιεί». Ο ένας συμμετέχοντας (QMSCert) σχολίασε ότι η συγκεκριμένη απαίτηση υφίσταται και στην περίπτωση χρήσης διάταξης απομακρυσμένης ηλεκτρονικής υπογραφής ή σφραγίδας. Η ΕΕΤΤ κάνει δεκτό και αυτό το σχόλιο. Κατά συνέπεια, η πρώτη παράγραφος τροποποιείται κατάλληλα.

2. Αναφορικά με τη δεύτερη παράγραφο, η ΕΕΤΤ αναγνωρίζει ότι, παρά την υποχρέωση του άρθρου 30, παρ. 2 του Κανονισμού eIDAS, δεν κοινοποιούνται πάντα οι πιστοποιήσεις των ΕΔΔΥ από τα Κράτη Μέλη, με αποτέλεσμα να υπάρχει περίπτωση ο κατάλογος που δημοσιεύει η Επιτροπή να μην είναι πλήρης. Για το λόγο αυτό, η συγκεκριμένη παράγραφος τροποποιείται κατάλληλα.

3. Διαπιστώνεται ότι μετά τις αλλαγές στις δύο παραγράφους του άρθρου αυτού, πρέπει να αλλάξει ο τίτλος του, ώστε να αντιστοιχεί στο περιεχόμενό του. Κατά συνέπεια, ο τίτλος του άρθρου αλλάζει σε «Απαιτήσεις για τις ΕΔΔΥ».

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

4. Τέλος, ένας συμμετέχοντας (QMSCert) σχολίασε ότι πρέπει να εισαχθούν υποχρεώσεις για την περίπτωση που χρησιμοποιείται αυτοματοποιημένη υπηρεσία απομακρυσμένης εγκατάστασης πιστοποιητικών προτείνοντας αφενός την υποχρέωση του εγκεκριμένου ΠΥΕ να αναγνωρίζει την ΕΔΔΥ που χρησιμοποιεί ο αιτών και να περιορίζει τη χρήση της υπηρεσίας μόνο στις αποδεκτές ΕΔΔΥ και αφετέρου την εξασφάλιση ορθής ενημέρωσης του συνδρομητή για τις ενέργειες στις οποίες πρέπει να προβεί ώστε να εκδοθεί το εγκεκριμένο πιστοποιητικό του. Ένας άλλος συμμετέχοντας (GUnet) πρότεινε η δυνατότητα αυτή να περιοριστεί μόνο σε ΕΔΔΥ που υποστηρίζουν από τον κατασκευαστή τους απομακρυσμένο κρυπτογραφικό έλεγχο στο δημιουργηθέν ιδιωτικό κλειδί (remote key attestation) καθώς και να απαγορευτεί η χρήση τέτοιων μεθόδων όταν η ΕΔΔΥ μπορεί να προσομοιωθεί με εικονική τοπική συσκευή με αποτέλεσμα το ζεύγος κλειδιών να δημιουργηθεί σε λογισμικό, παραβιάζοντας τις απαιτήσεις του Κανονισμού eIDAS. Η ΕΕΤΤ κάνει αποδεκτό το σχόλιο σχετικά με την εισαγωγή απαιτήσεων για την αυτοματοποιημένη υπηρεσία απομακρυσμένης εγκατάστασης πιστοποιητικών απορρίπτει όμως το σχόλιο σχετικά με την απαγόρευση μεθόδων που δεν πληρούν τις απαιτήσεις του Κανονισμού eIDAS καθώς η υποχρέωση συμμόρφωσης με τις απαιτήσεις προκύπτει άμεσα από τον Κανονισμό και την ευθύνη εξακρίβωσης της συμμόρφωσης φέρει ο Οργανισμός Αξιολόγησης της Συμμόρφωσης που διενεργεί τον έλεγχο και η ΕΕΤΤ. Για το λόγο αυτό η ΕΕΤΤ προσθέτει κατάλληλη διάταξη στην πρότασή της.

Άρθρο 11, παρ. 1

1. Ένας συμμετέχοντας (AthEx) προτείνει να τροποποιηθεί η πρόταση «Η έκδοση των εγκεκριμένων πιστοποιητικών πρέπει να γίνεται είτε τη στιγμή της παράδοσης της ΕΔΔΥ στο συνδρομητή, οπότε και…» σε «Η έναρξη ισχύος των εγκεκριμένων πιστοποιητικών πρέπει να γίνεται είτε τη στιγμή της παραλαβής της ΕΔΔΥ από το συνδρομητή και κατόπιν της επιβεβαίωσης των αναγραφόμενων στοιχείων του πιστοποιητικού…». Κατ' αρχάς, η επιβεβαίωση των αναγραφόμενων στοιχείων στο πιστοποιητικό είναι ευθύνη του συνδρομητή και όχι του παρόχου, προβλέπεται δε συνήθως στον Κανονισμό Πιστοποίησης που δημοσιεύει. Επιπλέον, η έναρξη της ισχύος ενός εκδοθέντος πιστοποιητικού δεν μπορεί να διασφαλιστεί ότι θα γίνει τη στιγμή της παραλαβής της ΕΔΔΥ από το συνδρομητή ή έστω αργότερα. Ο σκοπός της διάταξης είναι να εξασφαλίσει ότι το πιστοποιητικό δημιουργείται είτε όταν εγκαθίσταται στην ΕΔΔΥ που έχει στην κατοχή του ο συνδρομητής μέσω απομακρυσμένης υπηρεσίας εγκατάστασης ή κατά την παραλαβή της από τον ΠΥΕ είτε όταν ο συνδρομητής συνδέεται στην υπηρεσία

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

απομακρυσμένης υπογραφής για πρώτη φορά, διασφαλίζοντας έτσι ότι κανείς τρίτος δεν έχει τη δυνατότητα να υπογράψει αντί του συνδρομητή. Κατά συνέπεια, το σχόλιο απορρίπτεται.

2. Ένας συμμετέχοντας (QMSCert) σχολίασε αναφορικά με την πρώτη πρόταση της παραγράφου ότι τα πιστοποιητικά είναι δημόσια και ότι, λογικά, στην παρούσα νοούνται τα δεδομένα δημιουργίας της ηλεκτρονικής υπογραφής ή σφραγίδας. Ένας άλλος συμμετέχοντας (GUnet) σχολίασε ότι οι ΠΥΕ είναι υπεύθυνοι για την ασφαλή παράδοση των δεδομένων δημιουργίας υπογραφής στους δικαιούχους και τα δεδομένα αυτά είναι 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. Κατά την άποψή του, 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. Η ΕΕΤΤ διευκρινίζει ότι η πρόταση αυτή σκοπό έχει να καταστήσει σαφές ότι ένα εκδοθέν πιστοποιητικό πρέπει να βρίσκεται στην κατοχή του κατόχου του, με την έννοια ότι αυτός μπορεί να χρησιμοποιήσει την ΕΔΔΥ για να υπογράψει με αυτό, από την έναρξή του έως και τη λήξη του. Διατυπωμένο διαφορετικά, απαγορεύεται να υπάρχει εκδοθέν εγκεκριμένο πιστοποιητικό με ημερομηνία και ώρα έναρξης πριν την ημερομηνία και ώρα της παράδοσης της ΕΔΔΥ με τα δεδομένα δημιουργίας της ηλεκτρονικής υπογραφής ή σφραγίδας στον κάτοχό της. Η ΕΕΤΤ αποφασίζει να διαγράψει την πρόταση αυτή, καθώς το επιθυμητό πλαίσιο ορίζεται σαφώς στο υπόλοιπο της παραγράφου αυτής.

3. Δύο συμμετέχοντες (Adacom, Byte) σχολίασαν ότι δεν είναι κατανοητή η σύνδεση της έναρξης ισχύος του πιστοποιητικού με την παράδοση της ΕΔΔΥ ή την αρχική σύνδεση στην υπηρεσία απομακρυσμένης υπογραφής. Η ΕΕΤΤ έχει ήδη διευκρινίσει το λόγο σε απάντηση σε προηγούμενο σχόλιο. Οι ίδιοι συμμετέχοντες προτείνουν να γίνει πιο σαφής ο διαχωρισμός μεταξύ local-remote υπογραφής καθώς και την αναδιατύπωση της παραγράφου με δυνατότητα εκ νέου σχολιασμού. Η ΕΕΤΤ δεν θεωρεί ότι υπάρχει ανάγκη επαναδιατύπωσης του μέρους που αφορά στη local και στη remote υπογραφή και απορρίπτει το αίτημα για

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

εκ νέου σχολιασμό καθώς οι συμμετέχοντες είχαν τη δυνατότητα να προτείνουν το περιεχόμενο που θεωρούν αποδεκτό στο πλαίσιο της Δημόσιας Διαβούλευσης.

4. Ένας συμμετέχοντας (GUnet) σχολιάζει την πρόταση «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» αναφέροντας ότι αφενός είναι μεγάλη και δυσνόητη και αφετέρου δεν υποστηρίζει 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. Η ΕΕΤΤ δέχεται ότι η πρόταση είναι σχετικά μεγάλη αλλά όχι δυσνόητη. Σχετικά με την πρακτική της δημιουργίας δεδομένων δημιουργίας υπογραφής / σφραγίδας από τον ΠΕΥ εντός των ΕΔΔΥ και εκ των υστέρων χρήση τους για έκδοση εγκεκριμένου πιστοποιητικού, η ΕΕΤΤ σημειώνει ότι η πρότασή της δεν την αποκλείει αρκεί η έκδοση και εγκατάσταση του πιστοποιητικού να γίνεται τη στιγμή της παράδοσης της ΕΔΔΥ στο συνδρομητή. Ο ίδιος συμμετέχοντας σχολιάζει επίσης ότι η πρακτική που αναφέρεται ως «…τη στιγμή που, κατόπιν κατάλληλων ενεργειών του συνδρομητή, δημιουργείται στην ΕΔΔΥ το ζεύγος κλειδιών και εγκαθίσταται το εγκεκριμένο πιστοποιητικό…» έχει συγκεκριμένους και γνωστούς κινδύνους στην πλειονότητα των ΕΔΔΥ, οι οποίοι απομακρύνονται με χρήση πρακτικών που η συγκεκριμένη διατύπωση δεν υποστηρίζει, και προτείνεται να αλλάξει σε «…τη στιγμή που, κατόπιν κατάλληλων ενεργειών του συνδρομητή, δημιουργείται ή έχει δημιουργηθεί από τον ΠΥΕ στην ΕΔΔΥ το ζεύγος κλειδιών και εγκαθίσταται το εγκεκριμένο πιστοποιητικό…». Η ΕΕΤΤ αναγνωρίζει ότι ο σκοπός της παρούσας παραγράφου είναι να συνδέσει την ημερομηνία και ώρα έναρξης του εγκεκριμένου πιστοποιητικού με την κατοχή της ΕΔΔΥ από το συνδρομητή. Κατά συνέπεια, κάνει δεκτό το σχόλιο και αποσύρει το μέρος που αφορά στη δημιουργία των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας (ζεύγος κλειδιών).

5. Ένας συμμετέχοντας (GUnet) σχολιάζει ότι, στη φράση «…κατόπιν κατάλληλων ενεργειών του συνδρομητή, δημιουργείται στην ΕΔΔΥ το ζεύγος κλειδιών και…», το «ζεύγος κλειδιών» πρέπει να αντικατασταθεί

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

από «τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής». Η ΕΕΤΤ κάνει δεκτό το σχόλιο.

6. Ένας συμμετέχοντας (GUnet) σχολιάζει τη φράση «…η έκδοση του εγκεκριμένου πιστοποιητικού γίνεται τη στιγμή της αρχικής σύνδεσης και ενεργοποίησης της υπηρεσίας από το συνδρομητή» αναφέροντας ότι τα "short term certificates" δεν υποστηρίζονται από το άρθρο 11 και γενικότερα από το κείμενο της ΥΑ και προτείνει 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. Η ΕΕΤΤ αναγνωρίζει ότι η πρότασή της δεν είχε λάβει υπόψη τα "short term certificates" και για το λόγο αυτό προβαίνει σε σχετικές τροποποιήσεις. Παρόλα αυτά, οι διατάξεις της συγκεκριμένης παραγράφου είναι εφαρμοστέες και στα "short term certificates". Στην περίπτωση αυτή η σύνδεση στην υπηρεσία απομακρυσμένης υπογραφής διενεργείται από το χρήστη, είτε με άμεσο είτε και με έμμεσο τρόπο (π.χ. όταν ο χρήστης βρίσκεται ήδη στο περιβάλλον κάποιας υπηρεσίας που πρόκειται να κάνει χρήση του "short term certificate" για υπογραφή, η σύνδεση στην υπηρεσία απομακρυσμένης υπογραφής μπορεί να γίνει με αυτοματοποιημένο τρόπο χωρίς τη μεσολάβηση του χρήστη με κατάλληλη διεπαφή μεταξύ των δύο συστημάτων). Κατά συνέπεια, η ΕΕΤΤ δεν κάνει δεκτό το σχόλιο. Σε συνέχεια των ανωτέρω, η πρώτη παράγραφος του άρθρου 11 τροποποιείται κατάλληλα.

Άρθρο 11, παρ. 2

1. Ένας συμμετέχοντας (Adacom) ανέφερε ότι αναμένει αποσαφήνιση του κειμένου της παραγράφου 1 του ίδιου άρθρου προκειμένου να τοποθετηθεί σχετικά με την ημερομηνία και ώρα έναρξης. Η ΕΕΤΤ επισημαίνει ότι οι ενδιαφερόμενοι είχαν τη δυνατότητα να υποβάλουν τις απόψεις και τις προτάσεις τους στο πλαίσιο της Δημόσιας Διαβούλευσης.

2. Δύο συμμετέχοντες (GUnet, QMSCert) ανέφεραν ότι σε τεχνικό επίπεδο μπορεί να υπάρχουν μικρές αποκλίσεις λόγω προβλημάτων με το συγχρονισμό ρολογιών και προτείνουν να προβλεφθεί κάποια απόκλιση (λίγα λεπτά ο ένας και μερικές ώρες ο άλλος). Η ΕΕΤΤ αποδέχεται εν μέρη το σχόλιο και δέχεται απόκλιση έως 2 ώρες από τη Συγχρονισμένη Παγκόσμια Ώρα (UTC) καθώς θεωρεί ότι μεγαλύτερες αποκλίσεις δεν είναι λογικές για εγκεκριμένα πιστοποιητικά.

Άρθρο 11, παρ. 4

1. Ένας συμμετέχοντας (GUnet) αναφέρει ότι δεν κατανοεί πώς σχετίζεται η παράγραφος αυτή με το άρθρο 12. Πράγματι, πρόκειται για τυπογραφικό

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

λάθος καθώς το σωστό είναι το άρθρο 13 που αναφέρεται στο χρόνο υπογραφής. Δύο συμμετέχοντες (GUnet, QMSCert) αναφέρουν ότι δεν κατανοούν πώς μπορεί να εφαρμοστεί αυτή η διάταξη. Η ΕΕΤΤ αναγνωρίζει ότι, εφόσον ικανοποιούνται οι απαιτήσεις της παραγράφου 1, δεν είναι δυνατόν να υπάρξει εκδοθέν πιστοποιητικό με ημερομηνία και ώρα έναρξης πριν την ημερομηνία και ώρα παράδοσης που ο συνδρομητής έχει στην κατοχή του προς χρήση τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας. Στην περίπτωση όμως που, κατά παρέκκλιση των ανωτέρω, υπάρξει τέτοια περίπτωση, η ΕΕΤΤ κρίνει απαραίτητο να οριστεί το κατά πόσον η χρήση ενός τέτοιου πιστοποιητικού για υπογραφή ή σφράγιση είναι νόμιμη, αναγνωρίζοντας ότι τυχόν αμφισβήτηση δύναται να εξεταστεί μόνο από τα αρμόδια δικαστήρια. Κατά συνέπεια, η ΕΕΤΤ απορρίπτει το σχόλιο.

Άρθρο 11, *παρ.* 5

1. Αναφορικά με το πρώτο σημείο, ένας συμμετέχοντας (GUnet) ζητά να διευκρινιστεί το «τρίτο» μέρος ενώ ένας άλλος συμμετέχοντας (QMSCert) ζητά να διευκρινιστεί αν το «τρίτο» μέρος μπορεί να είναι και λογισμικό. Η ΕΕΤΤ διευκρινίζει ότι σκοπός της διάταξης είναι να διασφαλίσει ότι ο συνδρομητής μπορεί να διεκπεραιώσει όλες τις απαραίτητες ενέργειες στην περίπτωση υπηρεσίας απομακρυσμένης εγκατάστασης πιστοποιητικών σε ΕΔΔΥ είτε ο ίδιος είτε με την καθοδήγηση του ΠΥΕ (σημείο β). Δεν επιτρέπεται ο ΠΥΕ να δώσει οδηγίες σε τρίτο πρόσωπο προκειμένου να διεκπεραιώσει τη διαδικασία για λογαριασμό του συνδρομητή. Η RA/LRA ή κατάλληλα εξουσιοδοτημένοι συνεργάτες του ΠΥΕ δεν θεωρούνται «τρίτα» πρόσωπα. Βάσει των ανωτέρω, η ΕΕΤΤ κρίνει ότι η διάταξη είναι σαφής και δεν χρειάζεται τροποποίηση στο σημείο αυτό. Ένας συμμετέχοντας (GUnet) προτείνει την αντικατάσταση της φράσης «τη δημιουργία του ζεύγους κλειδιών» με «τη δημιουργία των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας». Η ΕΕΤΤ αποδέχεται το σχόλιο και τη διόρθωση. Τέλος, ο ίδιος συμμετέχοντας επισημαίνει ότι, καθώς το εγκεκριμένο πιστοποιητικό είναι δημόσια πληροφορία, δεν φαίνεται να υπάρχει κάποιο ιδιαίτερο θέμα ασφάλειας αν τρίτο μέρος μεσολαβήσει για την εγκατάσταση αυτού στην ΕΔΔΥ του συνδρομητή. Η ΕΕΤΤ αποδέχεται το σχόλιο και προχωρά σε κατάλληλη διόρθωση.

2. Όλοι οι συμμετέχοντες υπέβαλαν σχόλια για το δεύτερο σημείο. Τρεις συμμετέχοντες (Adacom, AthEx, Byte) ζήτησαν να προβλεφθούν κι άλλοι τρόποι επικοινωνίας (email π.χ.). Η ΕΕΤΤ απορρίπτει το σχόλιο και διευκρινίζει ότι η διάταξη ορίζει τις ελάχιστες απαιτήσεις και οι πάροχοι είναι ελεύθεροι να παρέχουν κι άλλους τρόπους υποστήριξης

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

των συνδρομητών τους. Ένας συμμετέχοντας (GUnet) ανέφερε ότι η τεχνική υποστήριξη είναι ανταγωνιστικό πλεονέκτημα και κριτήριο επιλογής παρόχου από την πλευρά των συνδρομητών ενώ δεν υπάρχει ουσιαστικός τρόπος ελέγχου από τον ΟΑΣ της τήρησης αυτής της υποχρέωσης. Η ΕΕΤΤ θεωρεί ότι στην περίπτωση που ο πάροχος επιλέξει την παροχή υπηρεσίας απομακρυσμένης εγκατάστασης πιστοποιητικών τότε πρέπει να είναι σε θέση να υποστηρίξει και τηλεφωνικά τους συνδρομητές του προκειμένου να διασφαλίζεται η υποχρέωση του σημείου α) της παρούσας παραγράφου και, κατά συνέπεια, απορρίπτει το σχόλιο. Τέλος, ένας άλλος συμμετέχοντας (QMSCert) σχολίασε ότι η συγκεκριμένη απαίτηση δεν είναι τεχνολογικά ουδέτερη ενώ υπάρχει και θέμα αυξημένου κόστους που μπορεί να μεταφερθεί στο συνδρομητή. Η ΕΕΤΤ διευκρινίζει ότι η συγκεκριμένη διάταξη δεν αφορά στην υποδομή δημόσιου κλειδιού των παρόχων ή στον τρόπο τεχνικής υλοποίησης που αυτοί έχουν επιλέξει αλλά στο ελάχιστο επίπεδο υποστήριξης των συνδρομητών του όταν ο πάροχος έχει επιλέξει να παρέχει υπηρεσία απομακρυσμένης εγκατάστασης πιστοποιητικών. Όσον αφορά στο κόστος που μπορεί να επιβαρύνει τον τελικό καταναλωτή, η ΕΕΤΤ αναγνωρίζει ότι το όφελος από τη διασφάλιση ότι ο συνδρομητής είναι αυτός που εκτελεί τις ενέργειες που προβλέπονται στην υπηρεσία και όχι κάποιο άλλο πρόσωπο πρέπει να είναι σταθμιστεί με βάση το τελικό κόστος στον καταναλωτή. Κατά συνέπεια, έχοντας σαν στόχο ένα ελάχιστο επίπεδο υπηρεσίας, η ΕΕΤΤ τροποποιεί τη διάταξη ώστε η τηλεφωνική γραμμή να είναι διαθέσιμη τουλάχιστον τις εργάσιμες ημέρες και 4 ώρες ημερησίως.

Άρθρο 12

1. Η ΕΕΤΤ κρίνει ότι εκτός από τον καθορισμό των περιορισμών που ισχύουν σχετικά με τη διάρκεια ισχύος εγκεκριμένων πιστοποιητικών, υφίστανται περιορισμοί και στα πιστοποιητικά των Αρχών Πιστοποίησης μιας ιεραρχίας που εκδίδει εγκεκριμένα πιστοποιητικά, όσον αφορά στη χρονική διάρκεια που οι αλγόριθμοι κρυπτογράφησης και κατακερματισμού θεωρούνται ασφαλείς. Κατά συνέπεια, προστίθεται τρίτη παράγραφος ως εξής:

   «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, παρ.1

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

1. Ένας συμμετέχοντας (QMSCert) σχολίασε ότι η συγκεκριμένη παράγραφος έχει πολύ σημαντικές νομικές προεκτάσεις «καθώς οποιοδήποτε ηλεκτρονικά υπογεγραμμένο έγγραφο δεν φέρει secure timestamp, έχει προσωρινή και αμφισβητούμενη ισχύ». Η ΕΕΤΤ διευκρινίζει ότι η παράγραφος προβλέπει ότι όταν δεν υπάρχει «αξιόπιστη πηγή» χρονικής πληροφορίας για το χρόνο υπογραφής του εγγράφου τότε ως χρόνος υπογραφής κατά την επικύρωση χρησιμοποιείται ο τρέχων χρόνος. Κατά συνέπεια, δεν αληθεύει ο ισχυρισμός ότι απουσία εγκεκριμένης χρονοσφραγίδας στο έγγραφο, αυτό έχει «προσωρινή και αμφισβητούμενη ισχύ» καθώς η ισχύς της υπογραφής ελέγχεται στο χρόνο που λαμβάνει χώρα η επικύρωση. Επομένως, το σχόλιο απορρίπτεται.

2. Ένας συμμετέχοντας (GUnet) σχολίασε ότι δεν ορίζεται ποιες είναι οι «αξιόπιστες πηγές» καθώς η εγκεκριμένη χρονοσφραγίδα αναφέρεται ως παράδειγμα, με αποτέλεσμα να μπορεί κάποιος να υποθέσει ότι η ώρα του υπολογιστή του υπογράφοντα ή μια μη εγκεκριμένη χρονοσφραγίδα αποτελούν «αξιόπιστες πηγές». Προτείνει δε να οριστεί μια λίστα με τις αξιόπιστες πηγές χρόνου. Η ΕΕΤΤ αποδέχεται το σχόλιο και διορθώνει το κείμενο της παραγράφου αλλάζοντας τη διατύπωση «(π.χ. εγκεκριμένη χρονοσφραγίδα, πρότυπο ETSI…)» σε «(εγκεκριμένη χρονοσφραγίδα)», δηλαδή αναφέροντας συγκεκριμένα τι θεωρείται ως «αξιόπιστη πηγή» πληροφορίας του χρόνου υπογραφής και αφαιρώντας την αναφορά στο πρότυπο για λόγους τεχνολογικής ουδετερότητας.

3. Μετά από σχόλιο που υπέβαλε ένας συμμετέχοντας (GUnet), η ΕΕΤΤ τροποποιεί την τελευταία πρόταση της παραγράφου ώστε να είναι σαφές ότι όταν δεν υπάρχει «αξιόπιστη πηγή» χρονικής πληροφορίας για το χρόνο υπογραφής του εγγράφου τότε ως χρόνος υπογραφής κατά την επικύρωση χρησιμοποιείται ο τρέχων χρόνος.

Άρθρο 13, παρ. 2

1. Δύο συμμετέχοντες (GUnet, QMSCert) εξέφρασαν αμφιβολίες κατά πόσον ηλεκτρονικά πρωτόκολλα χωρίς τεχνικές προδιαγραφές που μπορεί να επιτρέπουν τροποποιήσεις καταχωρίσεων στη βάση δεδομένων ή/και αλλαγή ημερομηνίας, μπορούν να θεωρούνται αξιόπιστα. Η ΕΕΤΤ αναγνωρίζει ότι υπάρχει αυτό το κενό στη διατύπωση της συγκεκριμένης παραγράφου και τροποποιεί κατάλληλα το κείμενο.

Άρθρο 13, παρ. 4

1. Ένας συμμετέχοντας (GUnet) ανέφερε ότι χρειάζεται να διευκρινιστεί αν κατά την επικύρωση πρέπει να ελέγχεται ότι οι αλγόριθμοι του άρθρου 14 ισχύουν τη στιγμή της επικύρωσης ή τη στιγμή της εκτιμώμενης υπογραφής του εγγράφου. Ζητά δε να διευκρινιστεί τι ισχύει στις

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

ακόλουθες περιπτώσεις: α) 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 β) αν η SHA1 υπογραφή δεν φέρει εγκεκριμένη χρονοσήμανση αλλά χρονοσήμανση από την ημερομηνία/ώρα του υπολογιστή του υπογράφοντα και γ) 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. Η ΕΕΤΤ διευκρινίζει ότι οι περιορισμοί του άρθρου 14 για την ισχύ των αλγορίθμων δημιουργίας ζεύγους κλειδιών και των συναρτήσεων κατακερματισμού ελέγχονται τη στιγμή της επικύρωσης. Κατά συνέπεια, αναφορικά με τις διευκρινίσεις που ζητήθηκαν για το αποτέλεσμα της επικύρωσης σε συγκεκριμένα παραδείγματα, αυτό θα είναι: α) άκυρη καθώς, βάσει του άρθρου 14, παρ. 2 ο αλγόριθμος SHA-1 γίνεται δεκτός έως την 1-6-2022 ενώ η επικύρωση λαμβάνει χώρα την 1-7-2022 β) έγκυρη αν η επικύρωση λάβει χώρα πριν την 1-6-2022, άκυρη αλλιώς και γ) έγκυρη με χρόνο υπογραφής την 1-7-2021 καθώς την ημερομηνία εκείνη ο αλγόριθμος SHA-1 είναι αποδεκτός και η νεότερη εγκεκριμένη χρονοσήμανση με SHA-256 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. Η ΕΕΤΤ συστήνει οι εκάστοτε υλοποιήσεις υπηρεσιών επικύρωσης να ακολουθούν το πρότυπο ETSI TS 119 102-1, στην εκάστοτε ισχύουσα έκδοσή του. Βάσει των ανωτέρω, κρίνεται ότι δεν χρειάζεται τροποποίηση του κειμένου της παραγράφου.

Άρθρο 14, παρ. 1

1. Ένας συμμετέχοντας (GUnet) σχολίασε ότι το χρονικό διάστημα των τριών μηνών για τη διακοπή χρήσης του αλγορίθμου είναι πολύ μικρό. Η ΕΕΤΤ δέχεται το σχόλιο και αυξάνει το διάστημα στους 6 μήνες (όπως ζήτησε και άλλος συμμετέχοντας (Adacom) σε σχόλιό του) λαμβάνοντας όμως υπόψη ότι έκτακτες καταστάσεις μπορεί να επιβάλουν την απόσυρση του αλγορίθμου σε συντομότερο χρονικό διάστημα. Ο ίδιος συμμετέχοντας σχολίασε ότι, εφόσον απαιτηθεί, η απόσυρση των Αρχών Πιστοποίησης πρέπει να γίνει προσεκτικά προκειμένου να μην προκληθούν προβλήματα σε υπογραφές που είναι έγκυρες. Η ΕΕΤΤ διευκρινίζει ότι η απόσυρση ενός αλγορίθμου γίνεται σε 2 επίπεδα. Στο πρώτο επίπεδο είναι ο πάροχος, ο οποίος ανακαλεί όσα τελικά πιστοποιητικά και όσες Αρχές Πιστοποίησης χρησιμοποιούν αυτό τον αλγόριθμο. Η διαδικασία αυτή δεν επηρεάζει το αποτέλεσμα της επικύρωσης για ήδη έγκυρες υπογραφές

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

και σφραγίδες που συνοδεύονται από εγκεκριμένη χρονοσφραγίδα. Σε δεύτερο επίπεδο, η ΕΕΤΤ αποσύρει όσες Αρχές Πιστοποίησης έχει ο πάροχος στον Κατάλογο Υπηρεσιών Εμπιστοσύνης, που χρησιμοποιούν αυτό τον αλγόριθμο. Εφόσον ο πάροχος έχει ολοκληρώσει το πρώτο βήμα και οι συνδρομητές του υπέγραφαν με χρήση εγκεκριμένης χρονοσφραγίδας, δεν θα επηρεαστεί το αποτέλεσμα της επικύρωσης από την απόσυρση της ΑΠ. Σε όλες τις άλλες περιπτώσεις το αποτέλεσμα της επικύρωσης θα είναι ότι η υπογραφή ή η σφραγίδα είναι άκυρη. Αυτό είναι και το σωστό αποτέλεσμα.

2. Η ΕΕΤΤ αναγνωρίζει ότι η πρόβλεψη της συγκεκριμένης παραγράφου για αυτόματη απόσυρση ενός αλγορίθμου όταν κρίνεται ως ακατάλληλος από το ETSI, είναι υπερβολική. Δεν είναι πάντα απαραίτητο αμέσως μόλις ένας αλγόριθμος κριθεί ακατάλληλος, να διακοπεί και η χρήση του. Το ίδιο αναφέρει κι ένας συμμετέχοντας (Adacom) σε σχόλιό του. Για παράδειγμα, ο αλγόριθμος SHA-1 θεωρείται ως ακατάλληλος από το 2005 αλλά ακόμα χρησιμοποιείται. Από την άλλη, ο αλγόριθμος MD5 θεωρείται ακατάλληλος και δεν πρέπει να χρησιμοποιείται γιατί δεν είναι ασφαλής. Άρα, πρέπει να υπάρχει ευελιξία αναφορικά με τον ορισμό της χρονικής στιγμής που πρέπει να εφαρμοστεί η απαγόρευση χρήσης ενός αλγορίθμου, λαμβάνοντας υπόψη το πρότυπο. Για το λόγο αυτό, προτείνεται να δοθεί στην ΕΕΤΤ η δυνατότητα να ορίζει με Απόφασή της αυτή τη χρονική στιγμή. Αλλιώς, θα απαιτείται η έκδοση Υπουργικής Απόφασης.

Άρθρο 14, παρ. 2

1. Ένας συμμετέχοντας (GUnet) ανέφερε ότι, όπως έχει διατυπωθεί, η υποχρέωση που επιβάλλει η παράγραφος αυτή αφορά μόνο στον εγκεκριμένο ΠΥΕ και τη χρήση του αλγορίθμου SHA-1 στα πιστοποιητικά των Αρχών Πιστοποίησης. Θεωρεί δε σωστό η υποχρέωση αυτή να επεκταθεί και στα εγκεκριμένα πιστοποιητικά που εκδίδονται στους συνδρομητές. Η ΕΕΤΤ κάνει δεκτό το σχόλιο και τροποποιεί την παράγραφο κατάλληλα.

2. Ο ίδιος συμμετέχοντας σχολίασε ότι η απαγόρευση χρήσης του αλγορίθμου SHA-1 δεν πρέπει να εφαρμοστεί σε πιστοποιητικά Αρχών Πιστοποίησης Ρίζας καθώς στα self-signed πιστοποιητικά δεν ελέγχεται η υπογραφή εντός του πιστοποιητικού αλλά μόνο το όνομα και το κλειδί (RFC 5280). Η ΕΕΤΤ κάνει δεκτό το σχόλιο με την προϋπόθεση ότι ο αλγόριθμος SHA-1 δεν χρησιμοποιείται σε άλλα στοιχεία της υπηρεσίας (π.χ. έκδοση CRL).

3. Δύο συμμετέχοντες (GUnet, QMSCert) ανέφεραν ότι θα πρέπει να διευκρινιστεί τι ισχύει με τα εγκεκριμένα πιστοποιητικά που θα έχουν

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

εκδοθεί με τη χρήση του αλγορίθμου SHA-1 την 1-6-2022, επισημαίνοντας ότι η μη ανάκλησή τους θα δημιουργήσει προβλήματα. Η ΕΕΤΤ κάνει δεκτό το σχόλιο, επισημαίνοντας ότι αφορά σε κάθε αλγόριθμο που δεν θα είναι πλέον αποδεκτός και όχι μόνο στον αλγόριθμο SHA-1, και τροποποιεί την πρώτη και τη δεύτερη παράγραφο του άρθρου κατάλληλα.

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

Επί του προτεινόμενου κειμένου της Υπουργικής Απόφασης που προβλέπεται στο αρ. 107, παρ. 34 του Ν.4727/2020

Άρθρο 2, παρ. 1

1. Δύο συμμετέχοντες (GUnet, QMSCert) σχολίασαν ότι το προτεινόμενο κείμενο της Υπουργικής Απόφασης δεν υποστηρίζει την αποδεκτή και ασφαλή λύση των πιστοποιητικών μικρής διάρκειας, τα οποία έχουν διαφοροποιήσεις κυρίως σε σχέση με τη δυνατότητα ανάκλησής τους. Η ΕΕΤΤ κάνει δεκτό το σχόλιο και αποφασίζει να εξαιρέσει από το πεδίο εφαρμογής της παρούσας τα πιστοποιητικά μικρής διάρκειας.

Άρθρο 2, παρ. 2

1. Δύο συμμετέχοντες (GUnet, QMSCert) επεσήμαναν ότι η αναφορά στο πρότυπο ETSI EN 319 412-2 είναι λανθασμένη και πρότειναν να αλλαχτεί στο ETSI EN 319 411-2, το οποίο παραπέμπει στο ETSI EN 319 411-1. Η ΕΕΤΤ κάνει δεκτό το σχόλιο.

2. Ένας συμμετέχοντας (GUnet) πρότεινε να γίνει υποχρεωτική η απάντηση "unknown" ή "revoked" των OCSP responders για άγνωστα πιστοποιητικά προκειμένου να αντιμετωπισθούν γνωστοί κίνδυνοι, σε συνδυασμό και με τον όρο OVR-6.6.3-02 του προτύπου ETSI EN 319 411-1. Η ΕΕΤΤ κάνει δεκτό το σχόλιο.

3. Ένας συμμετέχοντας (QMSCert) σχολίασε ότι, δεδομένης της συζήτησης σχετικά με την πρακτική απομάκρυνσης των ανακληθέντων εγκεκριμένων πιστοποιητικών από τη CRL όταν αυτά λήξουν και εφόσον α) δεν γίνεται χρήση της επέκτασης "ExpiredCertsOnCRL" και β) η πληροφορία παρέχεται από την υπηρεσία OCSP, θα ήταν καλύτερο να διευκρινιζόταν ότι η συνάφεια που αναφέρεται στην παράγραφο αυτή δεν αποκλείει την απομάκρυνση ληγμένων πιστοποιητικών από τη CRL (υπό τις παραπάνω προϋποθέσεις). Η ΕΕΤΤ διευκρινίζει ότι α) η CRL πρέπει να δίνει πληροφορία για την κατάσταση όλων των πιστοποιητικών, ληγμένων ή μη β) ομοίως η υπηρεσία OCSP και γ) πρέπει να υπάρχει συνάφεια μεταξύ των απαντήσεων της υπηρεσίας OCSP και της πληροφορίας που περιέχεται στη CRL, εφόσον παρέχονται και οι δύο. Επισημαίνεται, επιπλέον, ότι η χρήση της επέκτασης "ExpiredCertsOnCRL" (ETSI EN 319 411-2) είναι πλέον υποχρεωτική από το άρθρο 3, παρ. 2, σημ. α. Κατά συνέπεια, το σχόλιο δεν γίνεται δεκτό.

Άρθρο 3, παρ. 1

1. Ένας συμμετέχοντας (GUnet) σχολίασε ότι δεν είναι απαραίτητο να τηρείται η κατάσταση ανάκλησης και μετά τη λήξη του πιστοποιητικού για ορισμένες υπηρεσίες, όπως πιστοποιητικά για την επαλήθευση της

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

γνησιότητας ιστοτόπου, χρονοσφραγίδες, πιστοποιητικά υπηρεσίας συστημένης παράδοσης. Η ΕΕΤΤ κάνει δεκτό το σχόλιο μόνο όσον αφορά στα πιστοποιητικά για την επαλήθευση της γνησιότητας ιστοτόπου καθώς για τις υπόλοιπες περιπτώσεις που αναφέρει ο πάροχος θεωρεί ότι η πληροφορία πρέπει να είναι διαθέσιμη.

Άρθρο 3, παρ. 2

1. Η ΕΕΤΤ διαπιστώνει ότι η φράση «και να ενημερώνει για την κατάσταση κάθε ανακληθέντος πιστοποιητικού και μετά τη λήξη του» στο τέλος του σημείου α της παρούσας παραγράφου δεν είναι σωστή καθώς η απαίτηση είναι η υπηρεσία OCSP να ενημερώνει για την κατάσταση κάθε εκδοθέντος πιστοποιητικού, ληγμένου ή μη, ανακληθέντος ή όχι. Κατά συνέπεια, η φράση αυτή τροποποιείται κατάλληλα.

2. Δύο συμμετέχοντες (Byte, GUnet) σχολίασαν ότι το archive cutoff πρέπει να είναι προαιρετικό, όπως ορίζεται στο πρότυπο ETSI EN 319 411-2 και στο RFC6960 καθώς δεν είναι τεχνικά εφικτό να υπάρχει η συγκεκριμένη επέκταση σε όλες τις περιπτώσεις. Η ΕΕΤΤ κάνει δεκτό το σχόλιο και τροποποιεί το κείμενο ώστε η υποχρεωτικότητα να ισχύει μόνο στις περιπτώσεις που είναι τεχνικά εφικτό.

3. Δύο συμμετέχοντες (Adacom, GUnet) σχολίασαν ότι η πρώτη περίπτωση του δεύτερου σημείου της δεύτερης παραγράφου δεν μπορεί να ισχύει γιατί η διάρκεια ισχύος του πιστοποιητικού δεν μπορεί να υπερβαίνει την διάρκεια ισχύος της Αρχής Πιστοποίησης και έρχεται σε αντίθεση με το άρθρο 12, παρ. 1 του κειμένου της πρότασης για την Υπουργική Απόφαση του σημ. 31 του άρθρου 107 του ν.4727/2020 αλλά και με το RFC5280. Η ΕΕΤΤ κάνει δεκτό το σχόλιο και τροποποιεί κατάλληλα το κείμενο.

4. Δύο συμμετέχοντες (Adacom, Byte) σχολίασαν ότι η έκδοση τελικού OCSP response για κάθε εκδοθέν πιστοποιητικό δεν είναι υποχρεωτική από το πρότυπο (“may”) και ότι η σχετική υποχρέωση είναι τεχνικά απαιτητική. Η ΕΕΤΤ λαμβάνοντας υπόψη τα σχόλια των παρόχων, τροποποιεί το κείμενο ώστε η υποχρεωτικότητα να ισχύει μόνο στις περιπτώσεις που παρέχεται μόνο η υπηρεσία OCSP χωρίς να δημοσιεύεται παράλληλα CRL.

5. Ένας συμμετέχοντας (Byte) σχολίασε ότι στο ETSI EN 319 411-2 δεν υπάρχει απαίτηση για λήξη της τελευταίας CRL 31 Δεκεμβρίου 9999, 23:59:59. Η ΕΕΤΤ επέλεξε να περιλάβει αυτή την τιμή στην πρότασή της ώστε να ταυτίζεται με την τιμή που προτείνουν τα πρότυπα για την υπηρεσία OCSP. Κατά συνέπεια, το σχόλιο απορρίπτεται.

6. Ένας συμμετέχοντας (GUnet) σχολίασε ότι πρέπει να διορθωθεί η λέξη «πάροχος» στο τρίτο σημείο της δεύτερης παραγράφου και να αλλάξει σε «ΠΥΕ». Η πρόταση γίνεται δεκτή από την ΕΕΤΤ.

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

7. Ένας συμμετέχοντας (GUnet) ζήτησε να διευκρινιστεί στο τρίτο σημείο της δεύτερης παραγράφου 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». Η ΕΕΤΤ διευκρινίζει ότι η φράση αφορά στην υποχρέωση δημοσίευσης CRL ανά 24 ώρες, που πλέον δεν υφίσταται δεδομένου ότι η υπηρεσία σταματά να παρέχεται και κάνει δεκτό το σχόλιο απαλείφοντας τη σχετική πρόβλεψη.

8. Ένας συμμετέχοντας (GUnet) σχολίασε ότι δεν είναι κατανοητή η υποχρέωση του τέταρτου σημείου της δεύτερης παραγράφου. Η ΕΕΤΤ διευκρινίζει ότι, βάσει της υποχρέωσης αυτής, ένας πάροχος που δεν υλοποιεί τα οριζόμενα στα προηγούμενα σημεία τότε πρέπει να ενημερώσει κατάλληλα τα συστήματά του και να τα υλοποιήσει, στο βαθμό που είναι εφικτό, ακόμα και για τα ήδη εκδοθέντα πιστοποιητικά (αναδρομική ισχύς της διάταξης). Η ΕΕΤΤ τροποποιεί το κείμενο για λόγους μεγαλύτερης σαφήνειας και εισάγει πρόβλεψη αναφορικά με το χρονικό διάστημα υλοποίησης των απαιτούμενων αλλαγών.

9. Ένας συμμετέχοντας (Adacom) ζήτησε να διευκρινιστεί αν τα ανακληθέντα πιστοποιητικά πρέπει να περιλαμβάνονται στη CRL και μετά τη λήξη τους. Η ΕΕΤΤ διευκρινίζει ότι η πρόβλεψη του σημείου (i) της παραγράφου 2α αναφέρει ότι όλα τα ανακληθέντα πιστοποιητικά, ανεξάρτητα από το αν έχουν λήξει ή όχι, με την εξαίρεση των πιστοποιητικών για την επαλήθευση της γνησιότητας ιστοτόπου που προβλέπεται στην πρώτη παράγραφο, περιλαμβάνονται στη CRL.

Άρθρο 3, παρ. 3

1. Ένας συμμετέχοντας (GUnet) σχολίασε ότι εφόσον δεν πρόκειται για μία απαίτηση αλλά για περισσότερες είναι σωστό να αλλάξει το κείμενο από «την απαίτηση» σε «τις απαιτήσεις». Η ΕΕΤΤ κάνει δεκτό το σχόλιο και τροποποιεί το κείμενο σύμφωνα με αυτό.

2. Ο ίδιος συμμετέχοντας (GUnet) πρότεινε για λόγους διαφάνειας να οριστεί το CP/CPS ως το κείμενο στο οποίο θα δημοσιεύει ο ΠΥΕ τον τρόπο συμμόρφωσης με τις απαιτήσεις του άρθρου αυτού. Η ΕΕΤΤ κάνει δεκτό το σχόλιο και τροποποιεί το κατάλληλα.

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

Γενικά σχόλια

1. Ένας συμμετέχοντας (Adacom) ανέφερε ότι, δεδομένου ότι ορισμένα άρθρα απαιτούν αλλαγές στις υποδομές των παρόχων, κάποιες από τις οποίες είναι χρονοβόρες, πρέπει να οριστεί μια εύλογη μεταβατική περίοδος για την έναρξη ισχύος των δύο Υ.Α., ιδανικά ενός (1) έτους. Η ΕΕΤΤ έχει εισάγει στην πρότασή της σε διάφορα σημεία πρόβλεψη για διάστημα συμμόρφωσης.

2. Ένας συμμετέχοντας (GUnet) ανέφερε ότι πρέπει να εξεταστεί να επιτραπεί η δυνατότητα ασφαλούς δημιουργίας κλειδιών σε ΕΔΔΥ πριν την έκδοση πιστοποιητικών (secure key pre-generation) από τον ΠΥΕ και παράδοση στον Συνδρομητή έτσι ώστε ο Συνδρομητής να έχει στη διάθεσή του έναν αριθμό κλειδιών τα οποία ο ΠΥΕ έχει επιβεβαιώσει ότι δημιουργήθηκαν εντός ΕΔΔΥ και μπορούν να χρησιμοποιηθούν μελλοντικά για να συνδυαστούν με εγκεκριμένο πιστοποιητικό εγκεκριμένης ηλεκτρονικής υπογραφής/σφραγίδας. Η ΕΕΤΤ διευκρινίζει ότι μετά τις τροποποιήσεις στην πρώτη παράγραφο του άρθρου 11, η πρακτική αυτή επιτρέπεται.

3. Δύο συμμετέχοντες (GUnet, QMSCert) αναφέρουν ότι δεν υποστηρίζονται τα πιστοποιητικά μικρής διάρκειας. Η ΕΕΤΤ διευκρινίζει ότι, μετά την τροποποίηση του πεδίου εφαρμογής της Υπουργικής Απόφασης του σημείου 34, του άρθρου 107 του ν.4727/2020, τα πιστοποιητικά μικρής διάρκειας υποστηρίζονται χωρίς εμπόδια.

4. Ένας συμμετέχοντας (QMSCert) ανέφερε ότι «πέρα από την κατά περίπτωση αναφορά στα πρότυπα ETSI (κάτι το οποίο είναι έμμεση αναγνώρισή τους), θα μπορούσε να τα θέτει και ως τμήμα των απαιτήσεων που ελέγχονται κατά την επιθεώρηση. Για την διατήρηση της τεχνικής ουδετερότητας, θα μπορούσε να προβλέπεται επιθεώρηση "με άλλα ισοδύναμα σχήματα, για την ισοδυναμία των οποίων, το βάρος ευθύνης το φέρει ο ΟΑΣ"». Η ΕΕΤΤ διευκρινίζει ότι η συμμόρφωση με τις διατάξεις των προτύπων ETSI, που αναφέρονται στις προτάσεις του κειμένου των δύο Υπουργικών Αποφάσεων και που σχετίζονται με την υποχρέωση που επιβάλλεται σε κάθε σημείο που αυτά αναφέρονται, είναι υποχρεωτική. Με την εξαίρεση του προτύπου ETSI TS 119 312, που είναι υποχρεωτικό στο σύνολό του, στο μεγαλύτερο μέρος τους οι επιβαλλόμενες υποχρεώσεις αφορούν σε συγκεκριμένη κωδικοποίηση πεδίων και στον τρόπο που υλοποιείται η CRL και η υπηρεσία OCSP και, επομένως, δεν υπάρχει περιθώριο για άλλες ισοδύναμες υλοποιήσεις.

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

Κατά συνέπεια, η ΕΕΤΤ κρίνει ότι δεν απαιτείται να προστεθεί συγκεκριμένη πρόβλεψη στο κείμενο.

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