Αποτελέσματα της Πρόσκλησης Υποβολής Απόψεων σχετικά με τις Ηλεκτρονικές Υπογραφές, την Παροχή Υπηρεσιών Πιστοποίησης και την Εθελοντική Διαπίστευση.

1. ΕΙΣΑΓΩΓΗ

Σκοπός της παρούσας έκθεσης είναι η παρουσίαση των αποτελεσμάτων της Πρόσκλησης Υποβολής Απόψεων σχετικά με τις Ηλεκτρονικές Υπογραφές, σε θέματα που άπτονται της Παροχής Υπηρεσιών Πιστοποίησης και της Εθελοντικής Διαπίστευσης, μέσα από τη συνοπτική έκθεση των απαντήσεων των συμμετεχόντων.

Η πρόσκληση υποβολής απόψεων πραγματοποιήθηκε στο διάστημα από τις 12 έως τις 30 Νοεμβρίου 2001 και βασίστηκε στο σχετικό ερωτηματολόγιο της ΕΕΤΤ. Προς διευκόλυνση του αναγνώστη, το ανωτέρω ερωτηματολόγιο περιλαμβάνεται στο σύνολό του στο παρόν.

Στην Πρόσκληση Υποβολής Απόψεων συμμετείχαν, καταθέτοντας τις απόψεις τους, δεκαεπτά (17) φορείς, ο λεπτομερής κατάλογος των οποίων επισυνάπτεται στο Παράρτημα Ι. Προς αποφυγή τυχόν παρερμηνείας της ΕΕΤΤ, που θα οδηγούσε στην εξαγωγή λανθασμένων συμπερασμάτων, οι απαντήσεις στα επιμέρους ερωτήματα παρουσιάζονται όπως δόθηκαν από τους συμμετέχοντες.

2. ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ– ΑΝΑΓΝΩΡΙΣΜΕΝΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Ανάκληση – Ακύρωση Πιστοποιητικών

Η ΕΕΤΤ, προκειμένου να διασφαλιστεί η ασφάλεια των συναλλαγών, θεωρεί ότι θα πρέπει να προβλέπονται συγκεκριμένες περιπτώσεις ανάκλησης ή ακύρωσης των αναγνωρισμένων πιστοποιητικών. Ειδικότερα,

Ο πάροχος υπηρεσιών πιστοποίησης υποχρεούται να προβεί σε άμεση ανάκληση / ακύρωση ενός αναγνωρισμένου πιστοποιητικού, στις εξής περιπτώσεις:

α. μετά από αίτηση του κατόχου των δεδομένων δημιουργίας υπογραφής ή του νομίμως εξουσιοδοτημένου από αυτόν ατόμου,
β. εφόσον διαπιστωθεί από την ΕΕΤΤ ότι τα αναγνωρισμένα πιστοποιητικά περιέχουν ψευδείς ή ανακριβείς πληροφορίες ως προς το Παράρτημα Ι του πδ 150/2001,
γ. σε περίπτωση παύσης εργασιών του παρόχου υπηρεσιών πιστοποίησης

Ερώτημα 1: Διατυπώστε τα σχόλιά σας.
Θεωρείτε ότι στα πλαίσια του Κανονισμού που προτίθεται η ΕΕΤΤ να εκδώσει, θα πρέπει να προβλεφθούν και άλλες περιπτώσεις για τις οποίες θα επιβάλλεται η ανάκληση – ακύρωση πιστοποιητικού;

16/17 συμμετέχοντες συμφωνούν με τις προβλεπόμενες από την ΕΕΤΤ περιπτώσεις ανάκλησης - ακύρωσης πιστοποιητικών.

1/17 θεωρεί ότι τα θέματα αυτά θα πρέπει να απαντηθούν αφού είναι γνωστές οι αποφάσεις και ρυθμίσεις στα υπόλοιπα ερωτήματα.

2/17 συμμετέχοντες τις θεωρούν επαρκείς, ενώ οι υπόλοιποι προτείνουν και άλλες περιπτώσεις στις οποίες πρέπει να επιβάλλεται / προβλέπεται η ανάκληση – ακύρωση πιστοποιητικού και συγκεκριμένα:

- Στις περιπτώσεις που η ανάκληση προβλέπεται ρητά είτε στον "Κανονισμό Πιστοποίησης" (CPS) του Παρόχου Υπηρεσιών Πιστοποίησης, είτε στην Πολιτική του συγκεκριμένου Πιστοποιητικού (Certification Policy) είτε στην σύμβαση και τις ιδιαίτερες συμφωνίες που έχουν συναφθεί μεταξύ του Παρόχου και του πιστοποιούμενου (2/17).
- Εφόσον πρόκειται για φυσικό πρόσωπο, στην περίπτωση θανάτου, (1/17).
- Εφόσον διαπιστωθεί ότι το αναγνωρισμένο πιστοποιητικό χρησιμοποιήθηκε για να τελεστεί αξιόποινη πράξη (2/17). Κατά μία άποψη θα πρέπει να υπάρχει τελεσίδικη δικαστική απόφαση εναντίον του κατόχου του πιστοποιητικού, ή κατά άλλη άποψη (1/17) η ανάκληση επιβάλλεται εάν ο κάτοχος του πιστοποιητικού καταδικάστηκε για παραβίαση της ισχύουσας νομοθεσίας με αμετάκλητη δικαστική απόφαση.

- Όταν δηλώνεται κλοπή ή καθ'οιονδήποτε τρόπο απώλεια ή έκθεση του πιστοποιητικού ή /και ακόμα στοιχείων βάση των οποίων αυτό εκδίδεται (1/17).
- Αυτόματα από τον πάροχο υπηρεσιών πιστοποίησης:

  -με το πέρας του καθορισμένου χρόνου ισχύος του συγκεκριμένου πιστοποιητικού (4/17) ή των δεδομένων δημιουργίας υπογραφής που αντιστοιχούν σε αυτό (1/17),

  -αν το φυσικό ή νομικό πρόσωπο στο όνομα του οποίου έχει εκδοθεί το πιστοποιητικό δεν ανταποκρίνεται σε συμβατικούς όρους παροχής της υπηρεσίας, σύμφωνα με το Συμφωνητικό Συνδρομητή (4/17),

  -αν έχει λήξει το Συμφωνητικό Συνδρομητή με τον συνδρομητή ή ο πάροχος υπηρεσιών πιστοποίησης κατά τον έλεγχο της αίτησης απάντησης πιστοποιητικού έχει λόγο να πιστεύει πως είναι λάθος κάποιο ουσιώδες στοιχείο (1/17).
- Εφόσον διαπιστωθούν προβλήματα δυσλειτουργίας του συστήματος του παρόχου και ειδικότερα σε περίπτωση που ο πάροχος διαπιστώσει ότι έχει θιγεί η αξιοπιστία του συστήματος πληροφορικής με αποτέλεσμα να επηρεάζεται και η αξιοπιστία του αναγνωρισμένου πιστοποιητικού (1/17).
- Μετά από αίτηση τρίτου (ή νομίμως εξουσιοδοτημένου αντιπροσώπου του) που διαβεβαίωσε μια ιδιότητα ή ένα χαρακτηριστικό (attribute) του κατόχου των δεδομένων δημιουργίας υπογραφής, εφόσον αυτή η ιδιότητα ή το χαρακτηριστικό περιλαμβάνεται στα δημοσιοποιούμενα στοιχεία του αναγνωρισμένου πιστοποιητικού και έπαψε να υπάρχει ή μεταβλήθηκε (3/17).
- Οι συνδρομητές πρέπει επίσης να έχουν την υποχρέωση να ζητήσουν ανάκληση του πιστοποιητικού τους εάν τα ιδιωτικά τους κλειδιά έχουν χαθεί, κλαπεί, έχουν εκτεθεί σε πιθανό ή υπαρκτό κίνδυνο, ή εάν το PIN μέσω του οποίου οι συνδρομητές έχουν πρόσβαση στο ιδιωτικό τους κλειδί έχει εκτεθεί σε κίνδυνο ή/και οι πληροφορίες που υπάρχουν στο πιστοποιητικό δεν είναι ακριβείς ή έχουν αλλάξει (1/17).
- Εάν διαπιστωθεί από τον πάροχο υπηρεσιών πιστοποίησης ότι το ιδιωτικό κλειδί του (του πάροχου) έχει γίνει γνωστό / διαδοθεί σε τρίτους (5/17). Τρεις από τους ανωτέρω θεωρούν ότι αρκεί και η πιθανότητα διακύβευσης της μυστικότητας του προσωπικού κλειδιού του παρόχου υπηρεσιών πιστοποίησης που εκδίδει αναγνωρισμένα πιστοποιητικά (Certification Authority – CA) ή κατά έναν από αυτούς και της αρχής καταχώρησης (RA).
- Εάν διαπιστωθεί από τον πάροχο υπηρεσιών πιστοποίησης ότι το ιδιωτικό κλειδί του κατόχου έχει γίνει γνωστό / διαδοθεί σε τρίτους (4/17). Κατά δύο από αυτούς αρκεί και πιθανή διακύβευση της μυστικότητας του προσωπικού κλειδιού του κατόχου του πιστοποιητικού.
- Πιθανή ή αποδεδειγμένη διακύβευση της μυστικότητας του μέσου αποθήκευσης (π.χ. σκληρός δίσκος, smart card) του προσωπικού κλειδιού του κατόχου του πιστοποιητικού.(1/17) Το ίδιο ισχύει και σε περίπτωση απώλειας του μέσου διαπίστευσης (π.χ. smart card) (1/17).

- Ο κάτοχος του πιστοποιητικού αποσύρεται ή δεν πληροί πλέον τις προϋποθέσεις συμμετοχής στο πρόγραμμα υποδομής δημοσίων κλειδιών (PKI) που διέπεται από την πολιτική πιστοποίησης του CA (1/17).
- Αλλαγή των προϋποθέσεων, έτσι ώστε η αίτηση πιστοποίησης να μην εγκρίνεται πλέον εάν επαναληφθεί (1/17).
- Ο κάτοχος του πιστοποιητικού ενεργεί με τρόπο που παραβιάζει την Πολιτική Πιστοποίησης (1/17).
- Σε οποιαδήποτε άλλη περίπτωση που το CA το θεωρεί σκόπιμο, προκειμένου να εξασφαλίσει την ακεραιότητα ή την ασφάλεια των υπηρεσιών του PKI ή των εφαρμογών και των υπηρεσιών που βασίζονται στο PKI (1/17).
- Αλλαγή του ονόματος, του κατόχου (1/17).
- Αλλαγή της συσχέτισης του κατόχου και του παρόχου πιστοποιητικών (πχ αν ένας εργαζόμενος πάψει να εργάζεται σε μια εταιρία) (1/17).
- Αν ο κάτοχος καθυστερεί ή υστερεί στο να τηρήσει τις υποχρεώσεις, όπως αυτές ορίζονται στο CPS του παρόχου πιστοποιητικών, λόγω κάποιας φυσικής καταστροφής, βλάβης στα υπολογιστικά και τηλεπικοινωνιακά του συστήματα ή για οποιοδήποτε άλλο παράγοντα εκτός του ελέγχου του και ο οποίος θέτει σε κίνδυνο τα δεδομένα κάποιου άλλου χρήστη, (1/17).
- Αν λήξει η συμφωνία μεταξύ κατόχου και παρόχου πιστοποιητικών (1/17).
- Αν λήξει η συμφωνία μεταξύ CA και RA (που αντιστοιχεί στον κάτοχο) (1/17)
- Αν το ζητήσει ο RA ή ο CA (1/17).
- Ο πάροχος της υπηρεσίας θα διατηρεί το δικαίωμα (μετά από συγκεκριμένες διαδικασίες ενημέρωσης που μπορεί να ορίσει η ΕΕΤΤ) να ανακαλέσει ή να ακυρώσει πιστοποιητικά που έχει εκδώσει σε φυσικά ή νομικά πρόσωπα σε περίπτωση οικονομικών εκκρεμοτήτων των προσώπων αυτών με τον πάροχο (1/17).
- Παύση Εργασιακής Σχέσης / Συνεργικής Σχέσης (Cessation of Operation) : Σε περίπτωση έκδοσης πιστοποιητικού με στόχο την πιστοποίηση της σχέσης ενός φυσικού προσώπου με κάποια εταιρεία ή οργανισμό θα πρέπει να ανακαλείται κατ' αίτηση, με την παύση της σχέσης αυτής (παραίτηση, μετακίνηση) (1/17).
- Ανάκληση παλαιότερου πιστοποιητικού, που βρίσκεται σε ισχύ, σε περίπτωση επανέκδοσης νέου (Superceded) (1/17)
- Εφόσον διαπιστωθεί ότι τα αναγνωρισμένα πιστοποιητικά περιέχουν ψευδείς ή ανακριβείς πληροφορίες ως προς το Παράρτημα Ι του πδ 150/2001 (έχει απαλειφθεί από το αρχικό κείμενο η έκφραση «από την ΕΕΤΤ»), το οποίο θα αποδεικνύεται βάσει συγκεκριμένων αποδεικτικών στοιχείων, π.χ. εγγράφων, οπότε από την στιγμή που θα λαμβάνει γνώση περί αυτού ο πάροχος είτε από την ΕΕΤΤ ως εποπτεύοντα φορέα είτε από τρίτο έχοντα έννομο συμφέρον, θα υποχρεούται να προχωρήσει σε ανάκληση / ακύρωση του πιστοποιητικού (1/17).

- Η ΕΕΤΤ έχει το δικαίωμα να ζητήσει την ακύρωση ή ανάκληση της ισχύος αναγνωρισμένων πιστοποιητικών σε περίπτωση που υπάρχουν αποδείξεις ότι αυτά είναι πλαστά, ή μη επαρκώς προστατευμένα και καθίσταται δυνατή η πλαστογράφησή τους, ή εφόσον οι μηχανισμοί ασφαλείας που έχουν προβλεφθεί για τη παραγωγή και υποστήριξη του απαιτούμενου κρυπτογραφικού υλικού (αλγόριθμοι, κλειδιά, key distribution,...), έχουν αποδειχθεί τεχνολογικά επισφαλείς (περιέχουν security flaws), καθιστώντας δυνατή και μη ανιχνεύσιμη την τροποποίηση έγκυρων ψηφιακών υπογραφών και των κειμένων που αυτές επικυρώνουν (1/17).

Σημείωση:

Προτείνεται παράλληλα η πρόβλεψη της περίπτωσης Προσωρινής Αναβολής Ισχύος Πιστοποιητικού (Certificate Hold), όταν ο κάτοχος κατηγορείται ή βαρύνεται με αδικήματα τα οποία δικαιολογούν την ανάκληση της ισχύος του πιστοποιητικού και μέχρι την πλήρη διαλεύκανση των καταστάσεων αυτών, ώστε μετά τη διαλεύκανση τους η πλήρης ισχύς του πιστοποιητικού να επανέρχεται (1/17). Κατά άλλη συναφή άποψη (1/17) πρέπει να προβλέπεται υπηρεσία ‘προσωρινής παύσης πιστοποιητικών’ (certificate suspension) (π.χ. για τις περιπτώσεις που απαιτείται περαιτέρω εξακρίβωση της ταυτότητας του αιτούντος την ανάκληση ή όταν υπάρχουν απλές ενδείξεις έκθεσης (compromise) των δεδομένων δημιουργίας υπογραφής και ωσότου αυτές ερευνηθούν).

Παύση Εργασιών Παρόχων Υπηρεσιών Πιστοποίησης

Η ΕΕΤΤ θεωρεί ότι σε περίπτωση παύσης των εργασιών ενός παρόχου, θα πρέπει να προβλέπονται συγκεκριμένες διαδικασίες με τις οποίες θα εξασφαλίζεται η συνέχιση των υπηρεσιών πιστοποίησης από άλλον πάροχο υπηρεσιών πιστοποίησης. Ειδικότερα:

Πριν την, για οποιονδήποτε λόγο, παύση των εργασιών του, ή εάν αυτό δεν είναι αντικειμενικά εφικτό αμέσως μετά την παύση, ο πάροχος υπηρεσιών πιστοποίησης έχει τις ακόλουθες υποχρεώσεις:

(α) προβαίνει σε άμεση γνωστοποίηση στην ΕΕΤΤ,

(β) ενημερώνει αμέσως και_εγγράφως τους κατόχους των πιστοποιητικών σχετικά με την παύση των εργασιών του καθώς και τη δυνατότητά τους να επιλέξουν είτε την ανάθεση των πιστοποιητικών που τους έχει εκδώσει, και τα οποία εξακολουθούν να ισχύουν, σε άλλο πάροχο υπηρεσιών πιστοποίησης επιλογής του κατόχου, είτε ελλείψει τέτοιου, σε άλλο πάροχο υπηρεσιών πιστοποίησης επιλογής του παρόχου. Σε περίπτωση παύσης εργασιών εθελοντικά διαπιστευμένου παρόχου υπηρεσιών πιστοποίησης, τα πιστοποιητικά ανατίθονται σε άλλο εθελοντικά διαπιστευμένο πάροχο υπηρεσιών πιστοποίησης. Σε περίπτωση παύσης εργασιών παρόχου υπηρεσιών πιστοποίησης που εκδίδει αναγνωρισμένα πιστοποιητικά, τα πιστοποιητικά ανατίθονται σε άλλο πάροχο υπηρεσιών πιστοποίησης που εκδίδει αναγνωρισμένα πιστοποιητικά ή σε εθελοντικά διαπιστευμένο πάροχο υπηρεσιών πιστοποίησης.

(γ) παραδίδει όλα τα σχετικά έγγραφα και στοιχεία, που τηρεί στο αρχείο του στον πάροχο υπηρεσιών πιστοποίησης, ο οποίος αναλαμβάνει τα πιστοποιητικά, σύμφωνα με τα ανωτέρω υπό (β).

(δ) σε περίπτωση μη εφαρμογής των ανωτέρω υπό β, προβαίνει σε άμεση ακύρωση των εν λόγω πιστοποιητικών, καταθέτοντας όλα τα έγγραφα και στοιχεία που τηρεί στο αρχείο του, προς φύλαξη, στην ΕΕΤΤ και, ενημερώνει τους συναλλασσομένους.

Ερώτημα 2: Συμφωνείτε με την προσέγγιση αυτή στην περίπτωση της παύσης εργασιών του παρόχου υπηρεσιών πιστοποίησης;
Πιστεύετε ότι υπάρχουν τεχνικές ή άλλες δυσκολίες για την υλοποίηση της διαδικασίας αυτής;
Θεωρείτε ότι υπάρχει εναλλακτική διαδικασία και, εάν ναι, ποια;

Η πλειοψηφία των συμμετεχόντων συμφωνεί με την προσέγγιση της ΕΕΤΤ (10/17).

1 από τους 10 αν και συμφωνεί με τη μεταφορά των πιστοποιητικών σε άλλο πάροχο, προτείνει διαφορετική διαδικασία από την προβλεπόμενη από την ΕΕΤΤ.

Ένα ποσοστό διαφωνεί (3/17).

Ένα ποσοστό δεν αποσαφηνίζει τη θέση του (3/17).

1 από τους 17 δεν απάντησε στο ερώτημα.

Τα προβλήματα που παρουσιάζονται είναι:

- Συμβατότητα των προϊόντων ηλεκτρονικών υπογραφών (5/17)
- Ανάληψη κόστους και ευθύνης από τον παύων τις εργασίες του πάροχο και το διάδοχό του (4/17)
- Ζητήματα αξιοπιστίας (1/17)
- Συνύπαρξη παλαιών και νέων πιστοποιητικών κατά τη μεταβατική περίοδο μεταφοράς των πιστοποιητικών (1/17)
- Αποκάλυψη ή απόσυρση ιδιωτικού κλειδιού του παρόχου που παύει τις εργασίες του στο νέο πάροχο[1](2/17)
- Δεν πρέπει να επιβληθεί στους παρόχους υποχρέωση ανάληψης πιστοποιητικών (1/17)
- Μεταφορά και τήρηση των αρχείων των πιστοποιητικών (1/17)

[1] Η καταστροφή του ιδιωτικού κλειδιού του παρόχου σημαίνει και ανάκληση των πιστοποιητικών των κατόχων. Αυτό δεν έρχεται σε αντίθεση με το (β) τμήμα της διαδικασίας που προτείνει η ΕΕΤΤ, απλώς διευκρινίζει ότι αντικατάσταση παρόχου από άλλο πάροχο συνεπάγεται ανάκληση και επανέκδοση των πιστοποιητικών των κατόχων και των υφιστάμενων παρόχων. Αυτή η διαδικασία αντικατάστασης είναι όμοια με αυτές που περιγράφουν στα CPSs τους γνωστοί CAs, όπως η Globalsign και η Verisign. Συμπληρωματικά προβλέπεται στις περιπτώσεις αυτές:
- Προειδοποίηση των κατόχων 90 ημέρες πριν την παύση των εργασιών του παρόχου
- Συνέχιση για ένα διάστημα των υπηρεσιών υποστήριξης πελατών
- Συνέχιση των υπηρεσιών ανάκλησης πιστοποιητικών ώστε να είναι διαθέσιμες οι λίστες με τα ανακληθέντα πιστοποιητικά (CRLs) ή να είναι προσβάσιμες οι online υπηρεσίες ελέγχου κατάστασης των πιστοποιητικών.

- Η τεχνολογία κρυπτογράφησης αποτελεί περιουσιακό στοιχείο του κατασκευαστή και δε δύναται να δημοσιοποιηθεί σε τρίτους (1/17)

Προτείνεται:

- Να αφήνονται τα πιστοποιητικά να λήγουν και απλά σε ένα συγκεντρωτικό κατάλογο ανακληθέντων πιστοποιητικών, που μπορεί να τηρείται στην ΕΕΤΤ, να ανακοινώνεται η πιθανή ανάκλησή τους (1/17)
- Πρώτα να γίνεται η μεταβίβαση σε άλλο πάροχο και ύστερα η παύση λειτουργίας (1/17)
- Επιλογή του παρόχου να αποφασίσει εάν θα παραχωρήσει τους πελάτες του μετά την παύση των εργασιών του (2/17)
- Θα πρέπει να προβλέπεται η διαδικασία μετάβασης των πιστοποιητικών στο CPS ή /και στο Συμφωνητικό Συνδρομητή (1/17)
- Αλληλοπιστοποίηση μεταξύ των παρόχων (cross certification) (4/17)
- Ακύρωση όλων των πιστοποιητικών του παρόχου που παύει τις εργασίες του και μη εξαναγκασμός των κατόχων να δεχτούν νέο πάροχο (1/17)
- Ο πάροχος πρέπει να ενημερώνει όχι μόνο την ΕΕΤΤ και τους κατόχους πιστοποιητικών αλλά και όλους τους παρόχους ή γενικότερα οποιονδήποτε συνδέεται με αυτόν (1/17)
- Ο πάροχος θα πρέπει να αφαιρεί τη δυνατότητα από υπεργολάβους να δρουν εκ μέρους του σε διαδικασίες έκδοσης πιστοποιητικών (1/17)
- Η μέχρι εκείνη τη στιγμή χρήση των πιστοποιητικών που έχει εκδώσει ο πάροχος να διασφαλίζεται ότι δεν διακινδυνεύει να θεωρηθεί άκυρη ή μη γνήσια (1/17)
- Οι δραστηριότητες των παρόχων υπηρεσιών πιστοποίησης θα πρέπει να ασφαλίζονται για περιπτώσεις επιχειρηματικού κινδύνου (1/17)
- Η απάντηση του κατόχου του πιστοποιητικού θα πρέπει να δίνεται εντός συγκεκριμένου χρονικού διαστήματος, άλλως θα τεκμαίρεται η αποδοχή της ανάθεσης των πιστοποιητικών και της μεταφοράς των δεδομένων που αυτά εμπεριέχουν στον προτεινόμενο έτερο πάροχο (1/17)
- Ο πάροχος να παραδίδει όλα τα ψηφιακά τηρούμενα στοιχεία του που έχουν οποιαδήποτε σχέση με τις υπηρεσίες που προσέφερε κατά τη διάρκεια της λειτουργίας του, καθώς επίσης και κάθε εφεδρικό τους αντίγραφο (1/17)
- Ο πάροχος να παραμένει ποινικά και αστικά υπεύθυνος για οποιαδήποτε διαρροή ή παράνομη ή μη εξουσιοδοτημένη χρήση στοιχείων που περιήλθαν στην κατοχή του ως αποτέλεσμα των υπηρεσιών που προσέφερε κατά τη διάρκεια της λειτουργίας του (1/17)

3. ΕΘΕΛΟΝΤΙΚΗ ΔΙΑΠΙΣΤΕΥΣΗ ΤΩΝ ΠΑΡΟΧΩΝ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

Προϋποθέσεις για την Εθελοντική Διαπίστευση

Με την εθελοντική διαπίστευση θα διαπιστώνεται ότι ένας πάροχος υπηρεσιών πιστοποίησης πληροί τους όρους του ΠΔ 150/2001 και ειδικότερα ότι:

(α) ικανοποιεί τους όρους για την έκδοση αναγνωρισμένων πιστοποιητικών και ότι τα πιστοποιητικά που εκδίδει είναι αναγνωρισμένα και

(β) χρησιμοποιεί μόνο ασφαλείς διατάξεις δημιουργίας υπογραφής,

Τα ανωτέρω υπό α) και β) αποτελούν προϋποθέσεις χορήγησης της εθελοντικής διαπίστευσης, εντούτοις δεν περιορίζουν τον πάροχο να εκδίδει και μη αναγνωρισμένα πιστοποιητικά. Σε μία τέτοια περίπτωση ο χρήστης θα πρέπει να ενημερώνεται για το αν το πιστοποιητικό που εκδίδεται για λογαριασμό του είναι αναγνωρισμένο ή όχι.

Ερώτημα 3: Συμφωνείτε με τις ως άνω προϋποθέσεις;
Ποια διαδικασία πιστεύετε ότι θα πρέπει να ακολουθηθεί προκειμένου να εφαρμοστεί στην πράξη ο ως άνω διαχωρισμός μεταξύ μη αναγνωρισμένου και αναγνωρισμένου πιστοποιητικού;

2/17 δεν απάντησαν στο ερώτημα.

4/17 συμφωνούν συνολικά με το προτεινόμενο σχήμα. Ένας από αυτούς προτείνει ως πρόσθετη προϋπόθεση για την Εθελοντική Διαπίστευση Παρόχου Υπηρεσιών Πιστοποίησης (ΠΥΠ) την αναγγελία τήρησης αρχείου προς την Αρχή Προστασίας Προσωπικών Δεδομένων. Ένας άλλος θεωρεί ότι οι προϋποθέσεις που θα πρέπει να πληροί ο πάροχος αναγνωρισμένων πιστοποιητικών πρέπει να είναι ευθυγραμμισμένες με τα τέσσερα παραρτήματα του ΠΔ 150/2001, ενώ κάθε διαδικασία θα πρέπει να ορίζεται στο CPS του παρόχου.

Τα αναγνωρισμένα πιστοποιητικά θα πρέπει να πληρούν τις προϋποθέσεις που θέτουν τα πρότυπα: RFC3039 “Qualified Certificates Profile” [3] και TS 101 862 “Qualified Certificate Profile” [5] από το ETSI.

1/17 υποστηρίζει ότι τα κριτήρια για την Εθελοντική Διαπίστευση πρέπει να διαμορφώνονται σύμφωνα με τα εκάστοτε ισχύοντα Διεθνή Πρότυπα.

1/17 διαφωνεί συνολικά με το προτεινόμενο σχήμα. Συγκεκριμένα, επισημαίνει ότι στην Οδηγία 99/93 το «αναγνωρισμένο πιστοποιητικό» δεν συσχετίζεται με την εθελοντική διαπίστευση, αλλά αποκλειστικά και μόνο με τις απαιτήσεις του Παραρτήματος Ι. Η διαπίστωση, διασφάλιση και αναγνώριση της τήρησης των απαιτήσεων των παραρτημάτων Ι & ΙΙ δημιουργούν την ειδοποιό διαφορά μεταξύ

αναγνωρισμένου- και μη- πιστοποιητικού. Κατά την ίδια άποψη, η εθελοντική διαπίστευση αποσκοπεί αποκλειστικά στην επίτευξη βελτιωμένου επιπέδου παροχής υπηρεσιών πιστοποίησης (άρθρο 3 παρ. 2) και επιτυγχάνεται με τους δεδομένους μηχανισμούς διαπίστευσης που κάθε κράτος διαθέτει, θεωρώντας ότι στην Ελλάδα αρχή διαπίστευσης είναι το Εθνικό Συμβούλιο Διαπίστευσης (ΕΣΥΔ) (Νόμος 2231/94, όπως τροποποιήθηκε με το άρθρο 8 του νόμου 2542/98), από το πεδίο λειτουργίας του οποίου δεν εξαιρείται κανείς απολύτως τομέας ή φορέας πιστοποίησης είτε προϊόντων, είτε έργων, είτε όπως εδώ υπηρεσιών. Κατά την ίδια άποψη, η διαπίστευση των φορέων γίνεται σύμφωνα με τις Διεθνείς Οδηγίες – ISO Guides, τα πρότυπα της σειράς ΕΛΟΤ ΕΝ 45000, κριτήρια των οργανισμών WELAC, WECC, EAC αλλά και τους κανονισμούς του ΕΣΥΔ.

2/17 διαφωνούν με τον διαχωρισμό, υποστηρίζοντας ότι ένας Πάροχος που είναι διαπιστευμένος πρέπει να εκδίδει μόνο αναγνωρισμένα πιστοποιητικά. Ο ένας επικαλείται λόγους αποφυγής σύγχυσης και ο άλλος λόγους ασφάλειας των συναλλαγών και προστασίας του καταναλωτή γενικότερα, οι οποίοι δεν ικανοποιούνται με την πρόβλεψη υποχρέωσης του παρόχου να ενημερώνει το χρήστη, ούτε με την άσκηση κατασταλτικού ελέγχου από την Εποπτεύουσα Αρχή.

6/17 δεν συμφωνούν με την προϋπόθεση υπό (β), δηλ. ο εθελοντικά διαπιστευμένος Πάροχος Υπηρεσιών Πιστοποίησης (ή Πάροχος) να χρησιμοποιεί μόνο ασφαλείς διατάξεις δημιουργίας υπογραφής (εφεξής α.δ.δ.υ).

Κατά την άποψη ενός εξ αυτών πρέπει να επιτρέπεται στον Πάροχο να χρησιμοποιεί και ασφαλείς διατάξεις δημιουργίας υπογραφής, μεταξύ άλλων μέσων που έχει εντάξει στην επιχειρηματική του δραστηριότητα, αλλά προϋποθέσεις για την Εθελοντική Διαπίστευση ενός ΠΥΠ θα πρέπει να είναι μόνο: 1) η αποδεδειγμένη κάλυψη όλων των προϋποθέσεων και των όρων του Παραρτήματος ΙΙ (όπως αυτοί θα εξειδικευτούν από τα σχετικά πρότυπα), και 2) η (υποχρέωση για) έκδοση τουλάχιστον ενός τύπου 'αναγνωρισμένου πιστοποιητικού' προς το κοινό με δυνατότητα χρήσης «α.δ.δ.υ.». Ο ίδιος συμμετέχων συμφωνεί εντούτοις ότι τα 'προϊόντα ηλεκτρονικής υπογραφής' (άρ. 2 περ. 12) ήτοι το software & hardware που χρησιμοποιεί ο Πάροχος για την προσφορά των υπηρεσιών του (π.χ. δημιουργίας και διάδοσης των πιστοποιητικών, δημοσίευσης καταλόγων ισχυρών και ανακληθέντων πιστοποιητικών, δημιουργίας κλειδιών και μεταφοράς σε «α.δ.δ.υ.», δημιουργίας πιστοποιητικών χρονοσήμανσης κ.λ.π.) πρέπει σε έναν διαπιστευμένο Π.Υ.Π. να αποτελούν 'ασφαλείς διατάξεις', επισημαίνοντας ότι κάτι τέτοιο προβλέπεται ήδη στην περίπτωση (στ΄) του Παραρτήματος ΙΙ.

Άλλος από τους ανωτέρω συμμετέχοντες διαφωνεί τόσο με την επιβολή στον Π.Υ.Π. της υποχρέωσης (ως 'προϋπόθεση' για την εθελοντική διαπίστευσή του) να «χρησιμοποιεί μόνο ασφαλείς διατάξεις δημιουργίας υπογραφής» (α.δ.δ.υ.), όσο και με την διατύπωση «… και ότι τα πιστοποιητικά που εκδίδει είναι αναγνωρισμένα», υποστηρίζοντας ότι αντικείμενο της εθελοντικής διαπίστευσης είναι η εκ μέρους της ΕΕΤΤ επιβεβαίωση της συμμόρφωσης (του ΠΥΠ) με τα κριτήρια του Παραρτήματος ΙΙ της Οδηγίας και του π.δ. προσαρμογής (όπως πιθανώς εξειδικευτούν περισσότερο από την ΕΕΤΤ). Σύμφωνα με την ίδια άποψη, η απαίτηση να εκδίδεται από τον ΠΥΠ τουλάχιστον ένα αναγνωρισμένο πιστοποιητικό που προβλέπει (με την έννοια ότι παρέχει την δυνατότητα και την διαθεσιμότητα σχετικών υπηρεσιών) και την χρήση

α.δ.δ.υ. (ανάλογα με την επιλογή του χρήστη ή τις εφαρμογές για τις οποίες προορίζεται το πιστοποιητικό), ως ελάχιστη προϋπόθεση για να γίνει αποδεκτός ένας ΠΥΠ στις περαιτέρω διαδικασίες για την εθελοντική διαπίστευση, θα ήταν αποδεκτή, αφού έτσι α) και προσδίδει νόημα στην εθελοντική διαπίστευση χωρίς να περιορίζει τις επιχειρηματικές επιλογές του ΠΥΠ, και β) εξασφαλίζει στον υποψήφιο συνδρομητή-κάτοχο δεδομένων δημιουργίας υπογραφής που απευθύνεται σε έναν εθελοντικά διαπιστευμένο ΠΥΠ ότι θα βρει σ' αυτόν -εφόσον το επιθυμεί- τον συνδυασμό υπηρεσιών 'αναγνωρισμένου πιστοποιητικού' και 'ασφαλούς διατάξεως δημιουργίας υπογραφής' που καλύπτει (μαζί με την -σχεδόν δεδομένη- χρήση 'προηγμένης ηλεκτρονικής υπογραφής') τις προϋποθέσεις για την απόκτηση μιας πλήρως ισότιμης με την χειρόγραφη 'αναγνωρισμένης ηλεκτρονικής υπογραφής' κατά το άρ. 3§1 του σχετικού π.δ. Στο ίδιο πλαίσιο τονίζεται ότι η επιβολή σε έναν ΠΥΠ προσθέτων δεσμεύσεων προκειμένου να διαπιστευτεί εθελοντικά θα ήταν αντίθετη με το φιλελεύθερο πνεύμα της κοινοτικής Οδηγίας.

Κατά την άποψη ενός άλλου, η (β) προϋπόθεση πρέπει να είναι εφαρμόσιμη μόνο για μία προηγμένη ηλεκτρονική υπογραφή που είναι βασισμένη σε αναγνωρισμένο πιστοποιητικό το οποίο δημιουργήθηκε μέσω ασφαλούς διάταξης δημιουργίας υπογραφής.

Κατά άλλη άποψη, οι προϋποθέσεις εθελοντικής διαπίστευσης θα πρέπει να συνδέονται με την έκδοση αναγνωρισμένων πιστοποιητικών και όχι με οποιουδήποτε είδους υποχρέωση χρήσης α.δ.δ.υ για την δημιουργία του ζεύγους κλειδιών από τον ίδιο ΠΥΠ σε ένα συνδρομητή, ενώ σύμφωνα με μια άλλη άποψη η διαδικασία που θα οδηγεί στη διαπίστευση θα πρέπει να εστιάζεται στις διαδικασίες έκδοσης και διαχείρισης των πιστοποιητικών και όχι στο ασφαλές ή όχι της διάταξης. Άλλος εκ των συμμετεχόντων υποστηρίζει ότι ο πάροχος υπηρεσιών πιστοποίησης πρέπει να έχει τη δυνατότητα να προσφέρει διαφόρων τύπων πιστοποιητικά, συμπεριλαμβανομένων των μη αναγνωρισμένων, τα οποία θα μπορούν να χρησιμοποιηθούν και σε ειδικότερες εφαρμογές που υπαγορεύονται από τις ανάγκες τις εκάστοτε αγοράς, αναγράφοντας όμως ευδιάκριτα τους ειδικούς όρους χρήσης (Certificate Practice Statement).

1/17 διακρίνει τα εξής πιθανά σχήματα: Την ύπαρξη μερών που προσφέρουν μόνο μέρος από το σύνολο των υπηρεσιών ενός ΠΥΠ, πχ υπηρεσίες εγγραφής ή "card personalization" ή υπηρεσία "hotline", είτε (πράγμα που θεωρεί συνετότερο) τη θέση κανόνων βάσει των οποίων το Σχήμα Εθελοντικής Διαπίστευσης περιλαμβάνει τέτοιου είδους προϋποθέσεις.

Σχετικά με την ακολουθητέα διαδικασία προκειμένου να εφαρμοστεί στην πράξη ο ως άνω διαχωρισμός μεταξύ μη αναγνωρισμένου και αναγνωρισμένου πιστοποιητικού:

8/17 δεν πρότειναν διαδικασία.

4/17 κάνουν παραπομπή σε σχετικά πρότυπα για το διαχωρισμό μεταξύ αναγνωρισμένων και μη αναγνωρισμένων πιστοποιητικών. Μεταξύ αυτών, 2/17

παραπέμπουν στο πρότυπο του ETSI RFC 3039 "Qualified Certificates Profile", 3/17 κάνουν αναφορά στο πρότυπο ETSI TS 101 862 "Qualified Certificate Profile", ενώ 2/17 προτείνουν το πρότυπο ETSI 101 456[2].

Κατά την άποψη ενός εκ των ανωτέρω συμμετεχόντων η διαδικασία διαχωρισμού ενός αναγνωρισμένου πιστοποιητικού συνδέεται με τον έλεγχο συμμόρφωσης με τα παραπάνω πρότυπα και τις διαφορές τους με ένα απλό X.509 πιστοποιητικό, καθώς και με τη συμμόρφωση με το ΠΔ 150/2001[3].

2/17 θεωρούν ότι, τα αναγνωρισμένα πιστοποιητικά πρέπει να φέρουν τίτλο που τα διακρίνει από άλλες κατηγορίες ή τύπους πιστοποιητικών. Ειδικότερα, κατά την άποψη του ενός πρέπει να γίνεται υποχρεωτικά αναφορά εντός του σχετικού πληροφοριακού πεδίου που προβλέπεται σε κάθε ψηφιακή υπογραφή και αφορά στη χρήση και ισχύ της σε σχέση με συγκεκριμένες εφαρμογές (π.χ. αναγνωρισμένο πιστοποιητικό για κάθε νόμιμη χρήση ή αποκλειστικά για e-commerce transactions με κυβερνητικούς φορείς).

1/17 τονίζει το ρόλο της ΕΕΤΤ για την ενημέρωση των χρηστών σχετικά με τους παρόχους που εκδίδουν πιστοποιητικά, ανά κατηγορία (αναγνωρισμένα, μη-αναγνωρισμένα) ενώ 1/17 υποστηρίζει ότι επαφίεται στον πάροχο να ενημερώνει τους χρήστες για τις ιδιότητες της κάθε διάταξης. Κατά άλλη άποψη (1/17) σε περίπτωση έκδοσης μη αναγνωρισμένων πιστοποιητικών θα πρέπει ο πάροχος να ενημερώνει τους καταναλωτές με σαφή τρόπο για τις διαφορές τους από τα αναγνωρισμένα πιστοποιητικά σε επίπεδο ασφάλειας και πιστοποίησης, ενώ παράλληλα η ΕΕΤΤ θα πρέπει να δημοσιοποιεί τους Εθελοντικά διαπιστευμένους παρόχους, οι οποίοι εκδίδουν αναγνωρισμένα πιστοποιητικά.

Η ΕΕΤΤ ως η Κορυφή της Ιεραρχίας των Εθελοντικά Διαπιστευμένων Παρόχων Υπηρεσιών Πιστοποίησης

Με το μηχανισμό εθελοντικής διαπίστευσης εξασφαλίζεται και επιβεβαιώνεται ένα βελτιωμένο επίπεδο παροχής υπηρεσιών.

Για την πιστοποίηση της εγκυρότητας των δεδομένων επαλήθευσης υπογραφής, απαιτείται να βρεθεί ένα ολοκληρωμένο μονοπάτι πιστοποίησης (certification path) έτσι ώστε ο αποστολέας που επιθυμεί να στείλει ένα ασφαλές μήνυμα σε κάποιον που πιστοποιείται από έναν άλλο πάροχο πιστοποίησης, να επαληθεύσει τη ταυτότητα όλων των παρόχων πιστοποίησης που μεσολαβούν μέχρι τον παραλήπτη. Για το λόγο αυτό, απαραίτητο είναι η ανάπτυξη σχέσης εμπιστοσύνης μέσα από τη δημιουργία ενός μοντέλου εμπιστοσύνης.

Η ΕΕΤΤ θεωρεί ότι μία πιθανή, οργανωτική δομή των παρόχων υπηρεσιών πιστοποίησης, είναι και η υλοποίηση ενός ιεραρχικού μοντέλου, όπου οι εθελοντικά διαπιστευμένοι πάροχοι θα βρίσκονται κάτω από έναν αναγνωρισμένο φορέα που θα

[2] Κατά την άποψη ενός, το ETSI 101 456 διαχωρίζει τα αναγνωρισμένα πιστοποιητικά από τα μη αναγνωρισμένα, βάσει του αν συμμορφώνονται με το παράρτημα I της οδηγίας της ΕΚ και βάσει του αν ο πάροχος συμμορφώνεται με το παράρτημα II της οδηγίας της ΕΚ.

[3] Ο ίδιος συμμετέχων προτείνει για την εφαρμογή της διαδικασίας διαχωρισμού, τον έλεγχο του CPS (όχι μόνο το επίπεδο ασφάλειας των διατάξεων αλλά όλης της υποδομής του παρόχου (δικτυακός εξοπλισμός, φυσική ασφάλεια, ασφάλεια προσωπικού κλπ), σύμφωνα με τα πρότυπα ασφάλειας και τα πρότυπα πολιτικών διαχείρισης πιστοποιητικών που αναφέρονται στην απάντηση του ερωτήματος 10.

αποτελεί την κορυφή της ιεραρχίας (Root Certification Authority). Η εμπιστοσύνη ανάμεσα στα μέλη της ιεραρχίας, θα ανακτάται μέσα από τη διαδικασία της εθελοντικής διαπίστευσης. Σε μία τέτοια περίπτωση, η ΕΕΤΤ, εκτός από την έκδοση διαπιστωτικής πράξης εθελοντικής διαπίστευσης, μπορεί να αναλάβει να λειτουργήσει ως η κορυφή της ιεραρχίας πιστοποιώντας τα δημόσια κλειδιά των εθελοντικά πιστοποιημένων παρόχων και εκδίδοντάς τα πιστοποιητικά τους. Οι εθελοντικά διαπιστευμένοι πάροχοι, με τη σειρά τους, θα πιστοποιούν τα κλειδιά των χρηστών τους. Η έκδοση των αναγνωρισμένων πιστοποιητικών από την ΕΕΤΤ θα αποτελεί ένα αποφασιστικής σημασίας, στοιχείο στην εξασφάλιση της ασφάλειας του συστήματος της πιστοποίησης.

Ερώτημα 4: Συμφωνείτε με τη λειτουργία της ΕΕΤΤ, ως η κορυφή των εθελοντικά διαπιστευμένων;
Στην περίπτωση υλοποίησης από την ΕΕΤΤ της λειτουργίας αυτής, πιστεύετε ότι η ΕΕΤΤ θα πρέπει να δημιουργεί τα δεδομένα δημιουργίας και επαλήθευσης υπογραφής του εθελοντικά διαπιστευμένου;

Αναφορικά με το Α' ερώτημα:
Η πλειοψηφία των συμμετεχόντων διαφωνεί με τη λειτουργία της ΕΕΤΤ ως κορυφής των εθελοντικά διαπιστευμένων παρόχων (10/17).

Ένα ποσοστό συμφωνεί (3/17).

Ένα ποσοστό δεν τοποθετείται (3/17).

1 από τους 17 τηρεί ουδέτερη στάση.

Τα προβλήματα που παρουσιάζονται είναι:

- Λόγοι σκοπιμότητας, νομιμότητας, αναρμοδιότητας, ασυμβίβαστου (3/17)
- Ανάγκη διαπίστευσης της ΕΕΤΤ ως Root (2/17)
- Καταπάτηση από την ΕΕΤΤ της αρχής της τεχνολογικής ουδετερότητας, δεδομένου ότι η ΕΕΤΤ, επιλέγοντας να γίνει Root CA, θα πρέπει να επιλέξει κάποια συγκεκριμένη τεχνολογία με βάση την οποία θα αναλάβει να παρέχει πιστοποίηση των δημοσίων κλειδιών των διαπιστευμένων παρόχων (1/17)
- Τεχνικές δυσκολίες (1/17), δεδομένου ότι η Root CA θα χρειαστεί να τοποθετηθεί στο λογισμικό και στις εφαρμογές όλων των τελικών χρηστών (όπως Microsoft Outlook και Explorer, Netscape Navigator, κλπ.) και σε περίπτωση που αυτό δε συμβεί, η αλυσίδα θα αποτύχει και η υπογραφή δεν θα είναι έγκυρη (1/17)
- Υψηλό κόστος (3/17)
- Μη υιοθέτηση του μοντέλου Root CA από τις περισσότερες χώρες στον κόσμο (2/17)
- Ζήτημα ασφάλειας, δεδομένου ότι η ΕΕΤΤ θα ευθύνεται για πράξεις και παραλείψεις των διαπιστευμένων παρόχων (single point of failure) (3/17)

- Ανάλογα με το CPS που θα ακολουθεί η κορυφή είναι πιθανόν να καταστεί απαγορευτική η διαπίστευση κάποιου παρόχου λόγω αντικρουόμενων πολιτικών (1/17)
- Δημιουργία κατάλληλης υποδομής (1/17)
- Ερωτηματικό αν οι εταιρείες υπηρεσιών πιστοποίησης θα αποδεχθούν κάτι τέτοιο (1/17)

Προτείνεται:

- Δημιουργία ηλεκτρονικού μητρώου των διαπιστευμένων από την ΕΕΤΤ παρόχων, προσιτό στους χρήστες του διαδικτύου (2/17)
- Αλληλοπιστοποίηση (cross-certification) των παρόχων (2/17)
- Δημιουργία κέντρων δια-πιστοποίησης (cross-certification centers) (1/17)
- Συνεργασία με τις αντίστοιχες αρχές των άλλων κρατών-μελών της Ε.Ε. και ιδίως με την Επιτροπή του άρθρου 9 της Οδηγίας 99/93 (1/17)
- Ανεξαρτησία των παρόχων και η εθελοντική διαπίστευση να είναι αποτέλεσμα ελέγχων και τήρησης διαδικασιών «εκτός δικτύου» (off-line) (1/17)
- Λειτουργία της ΕΕΤΤ ως Bridge CA (1/17)
- Κάθε εθελοντικά διαπιστευμένος πάροχος να έχει τη δυνατότητα διαπίστευσης άλλων μη αναγνωρισμένων παρόχων σε χαμηλότερο επίπεδο του ιεραρχικού μοντέλου (1/17)

Αναφορικά με το Β’ ερώτημα:
Μόνο 2 από τους 17 τοποθετήθηκαν στο ερώτημα. Ο ένας διαφώνησε επικαλούμενος ότι τα δεδομένα δημιουργίας και επαλήθευσης υπογραφής από την ΕΕΤΤ πρέπει να δημιουργούνται μόνο από τους κατόχους τους, ώστε να είναι οι μόνοι που θα έχουν γνώση και πρόσβαση στο μυστικό προσωπικό κλειδί. Ο άλλος πρότεινε η διαδικασία δημιουργίας των κλειδιών των παρόχων υπηρεσιών πιστοποίησης να γίνεται σε χώρο της ΕΕΤΤ (εφόσον γίνει Root CA) παρουσία τόσο του προσωπικού της ΕΕΤΤ, όσο και του παρόχου.

Εξέταση της Αίτησης για Εθελοντική Διαπίστευση από Φορείς εκτός της ΕΕΤΤ – Ορισμός των Φορέων

Στα πλαίσια της εξέτασης του φακέλου που υποβάλλει ο πάροχος που αιτείται την εθελοντική του διαπίστευση, η ΕΕΤΤ θα ελέγξει τη συμμόρφωση του παρόχου με τις προϋποθέσεις εθελοντικής διαπίστευσης. Βάσει του ΠΔ 150/2001, η ΕΕΤΤ δύναται να ορίσει δημόσιους ή/και ιδιωτικούς φορείς που θα αναλάβουν το εν λόγω έργο. Στην περίπτωση αυτή, η ΕΕΤΤ θα ορίσει τους φορείς αυτούς θέτοντας κριτήρια με τα οποία θα εξασφαλίζεται ότι διαθέτουν την απαραίτητη τεχνική κατάρτιση και εμπειρία για την πραγματοποίηση του ελέγχου.

Η ΕΕΤΤ θα συντάσσει κατάλογο με όλους τους κατά τα ανωτέρω οριζόμενους φορείς. Ο πάροχος δύναται να επιλέξει από τον κατάλογο, τον φορέα που επιθυμεί να εξετάσει τον φάκελό του.

Ο αιτών την εθελοντική διαπίστευση θα υποβάλλει το φάκελο της αίτησής του ενώπιον της ΕΕΤΤ, στην οποία θα γνωστοποιεί και το όνομα του φορέα που έχει επιλέξει από τον ανωτέρω κατάλογο. Εν συνεχεία και μετά την ολοκλήρωση του ελέγχου του φακέλου από το φορέα, ο τελευταίος θα υποβάλλει στην ΕΕΤΤ εισήγηση σε σχέση με τη συμμόρφωση του παρόχου προς τις προϋποθέσεις χορήγησης της εθελοντικής διαπίστευσης και η ΕΕΤΤ θα εκδίδει τη σχετική διαπιστωτική πράξη.

Ερώτημα 5: Συμφωνείτε με την υλοποίηση ενός τέτοιου σχήματος για την εξέταση της αίτησης της εθελοντική διαπίστευσης;
Ποια πιστεύετε ότι θα πρέπει να είναι τα κριτήρια με τα οποία η ΕΕΤΤ θα επιλέξει τους φορείς αυτούς και πως πιστεύετε ότι θα πρέπει να οργανωθεί η σχετική διαδικασία;
Θα εκδηλώνατε ενδιαφέρον για την ανάληψη μίας τέτοιας δραστηριότητας και, εάν ναι, κάτω από ποιες προϋποθέσεις;
Ποιος πιστεύετε ότι θα πρέπει να αναλάβει το κόστος εξετάσεως της αιτήσεως για εθελοντική διαπίστευση;
Διαφοροποιείται η απάντησή σας ανάλογα με το αν ο έλεγχος γίνεται από την ΕΕΤΤ ή από τρίτον φορέα; Αν ναι, πως;

1/17 δεν απάντησε καθόλου στο ερώτημα αυτό, ενώ 3/17 δεν διευκρίνισαν αν συμφωνούν ή όχι με την προτεινόμενη διαδικασία.

8/17 συμφωνούν με την υλοποίηση του προτεινόμενου από την ΕΕΤΤ σχήματος εξέτασης της αίτησης της εθελοντική διαπίστευσης[4].

2/17 θεωρούν ότι οι αιτήσεις των υποψήφιων Παρόχων Υπηρεσιών Πιστοποίησης θα πρέπει να ελέγχονται απ' ευθείας από την ΕΕΤΤ, η οποία θα εκδίδει σχετική διαπιστωτική πράξη στον υποψήφιο πάροχο μόνο μετά από την ολοκλήρωση και την θετική έκβαση του διενεργηθέντος ελέγχου. Η ΕΕΤΤ δύναται να χρησιμοποιεί ως υπεργολάβους τρίτους φορείς, (οι οποίοι δεν πρέπει να έχουν το δικαίωμα να είναι και οι ίδιοι πάροχοι υπηρεσιών πιστοποίησης) και οι οποίοι θα πληρούν συγκεκριμένα κριτήρια που θα τεθούν από αυτήν. Κατά την άποψη του ενός εκ των ανωτέρω, πρέπει να εξασφαλίζεται η εκπροσώπηση σε νομικό και τεχνικό επίπεδο και η φυσική παρουσία στελεχών της ΕΕΤΤ, καθ' όλη τη διάρκεια του ελέγχου.

1/17 θεωρεί ότι το προτεινόμενο "σχήμα" υποκατάστασης της ΕΕΤΤ στα καθήκοντά της ως φορέα διαπίστευσης επιδέχεται πολλές δυνατές παραλλαγές και ως εκ τούτου δεν είναι δυνατόν να αξιολογηθεί ενιαία. Διακρίνει τις περιπτώσεις ολικής και μερικής υποκατάστασης, θεωρώντας προφανές, στην περίπτωση που ο

[4] Κατά την άποψη ενός των συμμετεχόντων, η ΕΕΤΤ, ενεργώντας ως επικεφαλής του Εθνικού Συστήματος Εποπτείας (όχι διαπίστευσης) των παρόχων υπηρεσιών πιστοποίησης ηλεκτρονικών υπογραφών δύναται να χρησιμοποιήσει τρίτους φορείς ως εργαλεία για την διαπίστωση ύπαρξης των απαιτήσεων των Παραρτημάτων.

υποκατάστατος είναι εσωτερικός σύμβουλος της ΕΕΤΤ, ότι ο ιδιωτικός φορέας θα συνδέεται συμβατικά μόνο με την ΕΕΤΤ (π.χ. ως τεχνικός της σύμβουλος) και δεν θα έχει εξουσία να δραστηριοποιείται έναντι τρίτων ως φορέας διαπίστευσης. Κατά την ίδια πάντα άποψη, στην περίπτωση αυτή, δεν θα μπορεί να δέχεται "ιδίω ονόματι" τις αιτήσεις τους να διαπιστευτούν, ούτε να αμοίβεται από αυτούς κ.τ.λ., παρά μόνον για λογαριασμό της ΕΕΤΤ και εφόσον εξουσιοδοτηθεί προς τούτο. Ο ίδιος συμμετέχων εκφράζει εντούτοις αμφιβολίες ως προς τη νομιμότητα μιας τέτοιας ειδικής υπεξουσιοδότησης (κατά πόσο μια δημόσια αρχή (η ΕΕΤΤ) δικαιούται να εξουσιοδοτεί ιδιώτες για την είσπραξη των εσόδων της ή (να τους ορίζει) ως αντίκλητο για τις αιτήσεις που απευθύνονται σ' αυτήν).

1/17 θεωρεί ότι ο έλεγχος ικανοποίησης των προϋποθέσεων εθελοντικής διαπίστευσης θα πρέπει να γίνεται από τρίτους φορείς και όχι από την ΕΕΤΤ η οποία πρέπει να καταρτίσει μητρώο ελεγκτών με βάση δημόσια πρόσκληση ενδιαφέροντος, ενώ κατά άλλη άποψη (1/17), δεδομένου ότι τα αποτελέσματα του ελέγχου πρέπει να είναι τα ίδια ανεξάρτητα από τον πραγματοποιούντα τον έλεγχο, η δυνατότητα επιλογής φορέα ελέγχου δεν έχει νόημα.

Ως προς τα κριτήρια επιλογής φορέων,

4/17 δεν πρότειναν κριτήρια, (1/17 δεν απάντησε καθόλου στο ερώτημα), ενώ 2/17 προτείνουν να εφαρμοσθούν ελάχιστα κριτήρια, αντίστοιχα προς τα ελάχιστα κριτήρια που θέτει η Απόφαση 2000/709/ΕΚ για το διορισμό φορέων ελέγχου της συμμόρφωσης προς το παρ. ΙΙΙ, (ήτοι ανεξαρτησία, επαγγελματική αξιοπιστία, τεχνογνωσία, αμεροληψία κ.τ.λ.).

1/17 προτείνει ως κριτήρια την ανεξαρτησία, την αξιοπιστία και την τεχνική κατάρτιση και δευτερευόντως την εμπειρία, ή κατά άλλη άποψη (1/17) προηγούμενη εμπειρία και κύρος, ή κατά άλλη άποψη (1/17) το ενδιαφέρον, την εξειδικευμένη γνώση (expertise) και την προηγούμενη εμπειρία ή κατά άλλη άποψη (1/17) κατάλληλη τεχνολογική και διαδικαστική γνώση για την πραγματοποίηση τέτοιων ελέγχων ή κατά άλλη άποψη (1/17) οικονομική ευρωστία, τεχνική αξιοπιστία, εμπειρία καθώς και διάθεση κατάλληλα καταρτισμένου προσωπικού). Κατά την ίδια άποψη οι ειδικοί θα πρέπει να επιλέγονται βάσει των επαγγελματικών τους προσόντων σε τομείς που περιλαμβάνουν τεχνική, οργανωτική και νομική εξειδίκευση, ενώ εναπόκειται στην ΕΕΤΤ να επιλέξει είτε το διορισμό οποιουδήποτε πληροί τα ελάχιστα αυτά κριτήρια είτε τον καθορισμό ενός συγκεκριμένου αριθμού υποκατάστατων φορέων (έναν ή περισσότερους), στους οποίους και θα αναθέσει το έργο αυτό (είτε ως υπεξουσιοδοτημένους αυτοτελείς φορείς διαπίστευσης είτε ως απλούς τεχνικούς συμβούλους της ΕΕΤΤ), ενώ σημειώνεται ότι πρέπει να προβλεφθεί επίσης η συμμόρφωση προς τα διεθνώς αναγνωρισμένα πρότυπα.

1/17 υποστηρίζει ότι πρέπει να υπάρχει ασυμβίβαστο μεταξύ της ιδιότητας του ελεγκτή και αυτής του παρόχου πιστοποίησης, όπως επίσης και της οποιασδήποτε εταιρικής σχέσης με πάροχο πιστοποίησης ή της απασχόλησης προσωπικού παρόχου

πιστοποίησης, ή της ανάληψης έργου του παρόχου πιστοποίησης και ότι ο ελεγκτής δεν θα πρέπει να επιλέγεται ούτε να προτείνεται από τον υποψήφιο προς έλεγχο πάροχο πιστοποίησης αλλά από την ΕΕΤΤ, βάσει διαδικασίας εκδήλωσης ενδιαφέροντος, απευθυνόμενης προς τους ελεγκτές που έχουν καταχωρηθεί στο μητρώο (οι οποίοι πρέπει να έχουν αναγνωρισμένο κύρος), ενώ πρέπει να καθοριστούν δεσμεύσεις των ελεγκτών για τήρηση του απορρήτου των στοιχείων που περιέρχονται σε γνώση τους κατά την διαδικασία ελέγχου.

1/17 θεωρεί ότι τα κριτήρια / προϋποθέσεις που θα ακολουθήσουν οι ιδιωτικοί ή οι δημόσιοι φορείς για την αξιολόγηση ενός ΠΥΠ πρέπει να ορισθούν από την ΕΕΤΤ, προτείνοντας ως βασικό έγγραφο το CWA 14172: EESSI Conformity Assessment Guidance parts 1-3, σημειώνοντας ότι η ΕΕΤΤ πρέπει να επιβλέπει όλη την διαδικασία των προϋποθέσεων και να διατηρεί κατάλογο με τους διαπιστευμένους παροχείς υπηρεσιών πιστοποίησης.

Κατά άλλη άποψη (1/17) οι φορείς θα πρέπει να:

-ανήκουν στον ελεγκτικό χώρο και να είναι κοινώς αποδεκτοί και αναγνωρισμένοι για τις αρχές, τα ηθικά πρότυπα και τις διαδικασίες που ακολουθούν (μεγάλοι διεθνείς ελεγκτικοί οίκοι),

-απασχολούν ικανό αριθμό προσωπικού, το οποίο να είναι άρτια καταρτισμένο, με διεθνούς κύρους αναγνωρισμένες ικανότητες στον έλεγχο των πληροφοριακών συστημάτων καθώς και αποδεδειγμένη αντίστοιχη ελεγκτική προϋπηρεσία τα τελευταία χρόνια (συμπεριλαμβανομένης ελεγκτικής εμπειρίας σε αντίστοιχα προγράμματα διαπίστευσης παρόχων υπηρεσιών πιστοποίησης του εξωτερικού), προτείνοντας για την αναγνώριση των ελεγκτικών ικανοτήτων των εν λόγω φορέων, την διεθνή πιστοποίηση για ελεγκτές πληροφοριακών συστημάτων (Certified Information Systems Auditor – CISA) του παγκόσμιου οργανισμού Information Systems Audit and Control Association (ISACA, http://www.isaca.org),

Ένας άλλος εκ των συμμετεχόντων προτείνει ως κριτήρια την γνώση, σε βάθος, θεμάτων σχετικών με ηλεκτρονική υπογραφή και γενικότερα κρυπτογραφία, υποδομή δημοσίου κλειδιού, ανάλυση αδυναμιών δικτύων και συστημάτων κλπ, των προτύπων που αναφέρονται στο ερωτηματολόγιο της ΕΕΤΤ, ώστε να υπάρχει υποδομή για την αξιολόγηση, θεμάτων σχετικών με ασφάλεια πληροφοριακών συστημάτων και πολιτικές ασφάλειας, εμπειρία από παρόμοια έργα (μελέτες υποδομής δημοσίου κλειδιού (PKI), ασφάλειας δικτύων και συστημάτων, ανάλυση αδυναμιών δικτύων και συστημάτων κλπ), τεχνική κατάρτιση και εμπειρία για την πραγματοποίηση ελέγχου, καθώς και σε θέματα υπευθυνότητας (liability), ασφαλιστικών θεμάτων (insurance) που απαιτούνται για την παροχή υπηρεσιών δημοσίου κλειδιού (PKI), εκτεταμένη νομική εξειδίκευση σε θέματα σύνταξης και προσαρμογής πολιτικών ασφάλειας, CPS κλπ.

1/17 προτείνει τη λεπτομερή καταγραφή των προδιαγραφών, βάσει των οποίων θα πραγματοποιείται η διαπίστευση, προκειμένου ο ελεγκτικός φορέας να έχει αποδεδειγμένα τη γνώση, την ικανότητα και την εμπειρία να ελέγχει άλλες εταιρείες για την παροχή υπηρεσιών πιστοποίησης. Παράλληλα θεωρεί ότι πρέπει να εκδίδεται μια «άδεια ασκήσεως» με βάση τα εξής κριτήρια: Οι φορείς ελέγχου που θα ορίζονται

μόνο από την ΕΕΤΤ δεν θα έχουν την δυνατότητα να γίνουν εθελοντικά διαπιστευμένοι πάροχοι, οι εθελοντικά διαπιστευμένοι πάροχοι θα ελέγχονται σε τακτά χρονικά διαστήματα για λογαριασμό της ΕΕΤΤ από έναν πιστοποιημένο φορέα ελέγχου, οι εθελοντικά διαπιστευμένοι πάροχοι τους οποίους πιστοποιεί μόνο η ΕΕΤΤ μπορούν να παρέχουν ελεγκτικές υπηρεσίες σε μικρότερες εταιρείες οι οποίες λειτουργούν ως μη διαπιστευμένοι πάροχοι και βρίσκονται ιεραρχικά σε χαμηλότερο επίπεδο, ενώ οι εταιρείες ελεγκτών και διαπιστευμένων παρόχων θα πρέπει να έχουν δημοσιευμένο ισολογισμό και διαφάνεια ως προς τις συναλλαγές τους.

1/17 προτείνει ως κριτήρια επιλογής τα εξής:

-διαχείριση ποιότητας σύμφωνα με το πρότυπο EN 45001/ISO 17025, ως εργαστήριο εκτίμησης ή το EN 45011/12 ως φορέας πιστοποίησης,

-ικανότητα για την εκτίμηση συμμόρφωσης προϊόντων IT-security σύμφωνα με το ITSEC, CC, ή IT συστήματα διαχείρισης ασφαλείας πχ BS 7799, ενώ επισημαίνει ότι η πρώτη εργασία θα πρέπει να πραγματοποιηθεί υπό την επίβλεψη της ΕΕΤΤ με δικαίωμα της ΕΕΤΤ να ελέγξει την Έκθεση Συμμόρφωσης.

4/17 δεν ενδιαφέρονται να αναλάβουν ρόλο εξέτασης της συμμόρφωσης των παρόχων υπηρεσιών πιστοποίησης προς τις προϋποθέσεις εθελοντικής διαπίστευσης.

6/17 θα εκδήλωναν ενδιαφέρον για την ανάληψη μιας τέτοιας δραστηριότητας.

7/17 δεν διευκρίνισαν αν ενδιαφέρονται ή όχι.

12/17 θεωρούν ότι το κόστος της διαδικασίας διαπίστευσης πρέπει να το φέρει ο ενδιαφερόμενος Πάροχος Υπηρεσιών Διαπίστευσης (ο αιτών την Εθελοντική Διαπίστευση) (εξ ολοκλήρου ή κατά μία άποψη το μεγαλύτερο μέρος αυτού). Ένας από αυτούς σημειώνει ότι στο βαθμό που πρόκειται για αμοιβή «επιχείρησης κατά παραχώρηση της αρχής» είναι εύλογο και σκόπιμο να καθορίζονται σε κάθε περίπτωση τα όρια της παραπάνω αμοιβής από την εξουσιοδοτούσα αρχή ΕΕΤΤ, ενώ κατά συναφή άποψη, το κόστος της διαδικασίας ελέγχου, θα καθορίζεται από την ΕΕΤΤ (κατά άλλη άποψη η ΕΕΤΤ πρέπει να διαθέτει Επίσημο Τιμοκατάλογο) αλλά θα βαρύνει τον ελεγχόμενο. Κατά άλλη άποψη το κόστος αυτό είναι ανεξάρτητο από το αν η ΕΕΤΤ ή τρίτος για την ΕΕΤΤ αναλάβει την διενέργεια των ελέγχων και πρέπει να επιμερίζεται μεταξύ των φορέων αυτών για την κάλυψη των εξόδων των ελέγχων και των αναγνωρίσεων, στα διάφορα στάδιά τους. Άλλος εκ των συμμετεχόντων υποστηρίζει ότι το κόστος θα πρέπει να αντικατοπτρίζει την εμπλοκή της Ε.Ε.Τ.Τ. στη διαδικασία, θεωρώντας ότι οποιαδήποτε εμπλοκή άλλου φορέα δε θα πρέπει να βαρύνει τον οργανισμό που επιθυμεί να διαπιστευτεί. Ένας από τους συμμετέχοντες θεωρεί ότι η ΕΕΤΤ ή άλλοι κυβερνητικοί φορείς θα μπορούσαν να ενθαρρύνουν τους ΠΥΠ με το να μοιράζονται με αυτούς το σχετικό κόστος. Κατά άλλη συναφή άποψη το κόστος του ελέγχου θα πρέπει να βαρύνει τον ελεγχόμενο και δύναται να επιμεριστεί στα πιστοποιητικά που θα εκδίδει. Ενώ κατά μια άλλη άποψη το κόστος πρέπει να επιμερίζεται μεταξύ των φορέων αυτών για την κάλυψη των εξόδων των ελέγχων και των αναγνωρίσεων, στα διάφορα στάδιά τους. Μερικοί από τους ανωτέρω (5/17) συμφωνούν ότι η επιβάρυνση του αιτούντος με το κόστος

Εθελοντικής Διαπίστευσης είναι ανεξάρτητη από το αν ο έλεγχος γίνεται από την ΕΕΤΤ ή από οριζόμενο φορέα.

1/17 εκτιμά ότι το σχετικό κόστος θα είναι μεγάλο και σε περίπτωση που το επωμισθεί ο πάροχος, η επιβάρυνση της δραστηριότητας του ίσως οδηγήσει σε απώλεια του εμπορικού ενδιαφέροντος από την πλευρά των παρόχων.

4/17 δεν απάντησαν σχετικά με το ποιος πρέπει να αναλάβει το κόστος.

Έκδοση Αναγνωρισμένων Πιστοποιητικών Μόνο σε Περιβάλλον Ασφαλών Διατάξεων Δημιουργίας Υπογραφής

Η ΕΕΤΤ προτίθεται να επιβάλει την υποχρέωση στον εθελοντικά διαπιστευμένο να εκδίδει αναγνωρισμένα πιστοποιητικά σε φυσικά ή νομικά πρόσωπα μόνο όταν αυτά χρησιμοποιούν ασφαλείς διατάξεις δημιουργίας υπογραφής για την αποθήκευση των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής και τη δημιουργία της ψηφιακής τους υπογραφής.

Ερώτημα 6: Διατυπώστε την άποψή σας. Συμφωνείτε ότι ο εθελοντικά διαπιστευμένος πάροχος υπηρεσιών πιστοποίησης θα πρέπει να εκδίδει αναγνωρισμένα πιστοποιητικά σε φυσικά ή νομικά πρόσωπα *μόνο* όταν αυτά χρησιμοποιούν ασφαλείς διατάξεις δημιουργίας υπογραφής για την αποθήκευση των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής και τη δημιουργία της ψηφιακής τους υπογραφής;
Πιστεύετε ότι μπορεί να δημιουργηθούν προβλήματα από την επιβολή μίας τέτοιας υποχρέωσης; Αν ναι ποια;

Ένα μεγάλο ποσοστό (8/17) συμφωνεί[5] με την τοποθέτηση της ΕΕΤΤ ότι ο εθελοντικά διαπιστευμένος πάροχος υπηρεσιών πιστοποίησης θα πρέπει να εκδίδει αναγνωρισμένα πιστοποιητικά σε φυσικά ή νομικά πρόσωπα μόνο όταν αυτά χρησιμοποιούν ασφαλείς διατάξεις[6] δημιουργίας υπογραφής για την αποθήκευση των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής και τη δημιουργία της ψηφιακής τους υπογραφής.

Ένα ποσοστό (6/17) διαφωνεί με την ως άνω τοποθέτηση της ΕΕΤΤ[7].

Δεν τοποθετήθηκαν 2 από τους 17, ενώ 1 από τους 17 δε δε ξεκαθάρισε τη θέση του.

Τα προβλήματα που θίγονται είναι:

[5] Αναφέρθηκαν και συγκεκριμένα πλεονεκτήματα της προσέγγισης, όπως η επίτευξη υψηλότερου επιπέδου ασφαλείας κυρίως σε περιπτώσεις υποκλοπής και πλαστογράφησης. Επιπλέον επισημάνθηκε από έναν ότι ο πάροχος θα πρέπει να αποδεικνύει ότι συμμορφώνεται με τις σχετικές Οδηγίες της ΕΕ.
[6] 1 από τους 8 παρατήρησε ότι παρουσιάζεται ασάφεια όσον αφορά τον ορισμό του όρου «ασφαλείς διατάξεις»
[7] 1 από του 6 επικαλέστηκε το γεγονός ότι οι απαιτήσεις για τις ασφαλείς διατάξεις δημιουργίας υπογραφής περιγράφονται στην Οδηγία.

- Αντίθεση με το άρθρο 4 παρ. 1 του ΠΔ 150/2001 (1/17)
- Τεχνικά ανέφικτο και πολυπλοκότητα του συστήματος (2/17)
- Υπερβολικό κόστος (2/17)
- Ο εθελοντικά διαπιστευμένος πάροχος δεν έχει τη δυνατότητα να ελέγξει και να παρακολουθεί τις εκάστοτε τερματικές συσκευές που χρησιμοποιεί το κάθε φυσικό ή νομικό πρόσωπο που έχει συμβληθεί με αυτόν (1/17)

Προτείνεται:

- Να υπάρχει ως προϋπόθεση μόνο για τις προηγμένες ηλεκτρονικές υπογραφές του άρθρου 3 παρ. 1 του ΠΔ 150/2001 (1/17)
- Να υπάρχει υποχρέωση δέσμευσης του ΠΥΠ μέσω συμβολαίου με τους πελάτες του (1/17)
- Χρήση του κατάλληλου αλγόριθμου και του κατάλληλου μήκους κλειδιού, όπως αυτά προδιαγράφονται από τον πάροχο πιστοποιητικών, σύμφωνα με το TS 101 456 "Policy requirements for certification authorities issuing qualified certificates" του ETSI (1/17)

Να επιβεβαιώνεται στο CPS το γεγονός ότι ο κάτοχος κατέχει ασφαλή διάταξη δημιουργίας υπογραφής. (1/17)

Εξειδίκευση Προϋποθέσεων για την Εθελοντική Διαπίστευση

Το παράρτημα ΙΙ του ΠΔ 150/2001 θέτει μια σειρά από προϋποθέσεις (τεχνικές, οικονομικές κλπ.) που πρέπει να πληροί ο πάροχος που εκδίδει αναγνωρισμένα πιστοποιητικά. Στα πλαίσια της χορήγησης της εθελοντικής διαπίστευσης η ΕΕΤΤ, ή οι φορείς που θα οριστούν από αυτή – εφόσον προκριθεί μια τέτοια διαδικασία- θα πρέπει να ελέγξουν τη συμμόρφωση του αιτηθέντος την εθελοντική διαπίστευση με το Παράρτημα ΙΙ. Σε αρκετές περιπτώσεις οι όροι που περιλαμβάνονται στο Παράρτημα ΙΙ είναι γενικοί και δεν είναι σαφές με ποιο τρόπο ο πάροχος που αιτείται την εθελοντική του διαπίστευση θα αποδεικνύει τη συμμόρφωσή του με αυτούς.

Ερώτημα 7: Ποια είναι κατά την άποψή σας τα στοιχεία που θα πρέπει να προσκομίσει ο πάροχος προκειμένου να αποδείξει τη συμμόρφωσή του με τα κριτήρια του παραρτήματος ΙΙ του ΠΔ 150/2001;
Εκτιμάτε ότι θα πρέπει να ζητείται η συμμόρφωση και με άλλα στοιχεία και, εάν ναι, με ποια;

3/17 δεν απάντησαν στο ερώτημα αυτό.

1/17 παρέπεμψε γενικά στη διεθνή εμπειρία / πρακτική στο ζήτημα.

1/17 υποστήριξε ότι ο πάροχος θα πρέπει να αποδεικνύει συμμόρφωση με τις κοινοτικές οδηγίες. Άλλος (1/17) εκ των συμμετεχόντων θεωρεί αρκετή την υποβολή

μιας «Πολιτικής Ασφάλειας» (security concept) στην οποία περιγράφεται ο τρόπος πλήρωσης των προϋποθέσεων του πδ.[8]

1/17 θεωρεί ότι τα κριτήρια του Παραρτήματος ΙΙ εξειδικεύονται ικανοποιητικά από τα 'πρότυπα' ETSI 101 456 και CEN-CWA 14167-1, με περαιτέρω ανάγκη εξειδίκευσης από την ΕΕΤΤ συγκεκριμένων όρων και προτείνει για την απόδειξη της συμμόρφωσης του παρόχου με αυτά την προσκόμιση των παρακάτω στοιχείων:

α. κανονισμό πιστοποίησης (Certificate Practice Statement - CPS) του Παρόχου και (αναλόγως της αναλυτικότητας του Κανονισμού) τυχόν άλλα κείμενα σχετικά με τον έλεγχο και τις διαδικασίες της Πιστοποίησης,

β αποδεικτικά στοιχεία του Παρόχου περί της κατοχής και χρήσης 'προϊόντων ηλεκτρονικής υπογραφής' (Hardware-Software), που χρησιμοποιεί στις παρεχόμενες υπηρεσίες πιστοποίησης και που καλύπτουν τις απαιτήσεις και προδιαγραφές που ορίζει ο παραπάνω Κανονισμός (όπου θα φαίνεται ο τύπος των προϊόντων αυτών και οι τυχόν διαπιστεύσεις συμμόρφωσής τους σε ευρωπαϊκά ή διεθνή πρότυπα βάσει του Κανονισμού της ΕΕΤΤ),

γ. μία –τουλάχιστον- Πολιτική του Παρόχου που να αναφέρεται σε έκδοση 'Αναγνωρισμένου Πιστοποιητικού' με δυνατότητα χρήσης «ασφαλούς διάταξης δημιουργίας υπογραφής»,

δ. όλα τα έντυπα που προμηθεύεται ή υπογράφει ο συνδρομητής-πιστοποιούμενος κατά την διαδικασία εγγραφής του, ταυτοποίησής του και απόκτησης του παραπάνω 'αναγνωρισμένου πιστοποιητικού' (δηλαδή Συνδρομητική Σύμβαση, Φόρμες Αίτησης, Περίληψη όρων Κανονισμού Πιστοποίησης και Πολιτικής, Ενημερωτικό-εκπαιδευτικό Υλικό, κ.λ.π.),

ε. οποιοδήποτε άλλο έγγραφο κρίνεται απαραίτητο για την απόδειξη συμμόρφωσης σε επιμέρους όρους που δεν καλύπτονται από τα παραπάνω (π.χ. νομιμοποιητικά έγγραφα και αποδείξεις για την καταβολή του μετοχικού κεφαλαίου, άλλα έγγραφα σχετικά με την αξιοπιστία, το απασχολούμενο προσωπικό κ.λ.π.). Κατά την ίδια άποψη πρέπει να παρέχεται η δυνατότητα στον Πάροχο Υπηρεσιών Πιστοποίησης να αποδείξει τη συμμόρφωσή του στους όρους του Παραρτήματος ΙΙ του ΠΔ 150/2001, με κάθε πρόσφορο ή νόμιμο μέσο.

1/17 υποστηρίζει ότι θα πρέπει να θεωρηθεί ότι ο πάροχος πληροί κατ' αρχήν τις προϋποθέσεις εθελοντικής διαπίστευσης, οπότε εναπόκειται στους ελεγκτές να αναζητήσουν κατά την κρίση τους αποδείξεις περί του αντιθέτου. Αρκεί κατά τη διαδικασία ελέγχου, ο πάροχος να προσκομίσει τα απολύτως αναγκαία στοιχεία, εφόσον, συμπληρωματικά προς αυτά, παρέχει στους ελεγκτές διευκόλυνση πρόσβασης, κατ' απαίτηση, σε εγκαταστάσεις και στοιχεία του, με δυνατότητα προσφυγής στην ΕΕΤΤ για κάθε ενδεχόμενη διαφωνία μεταξύ παρόχου και ελεγκτή σχετικά με την πρόσβαση του τελευταίου σε εγκαταστάσεις ή στοιχεία του πρώτου.

[8] Ένας εκ των συμμετεχόντων ισχυρίσθηκε ότι διαθέτει ο ίδιος κατάλληλες διαδικασίες ώστε να μπορεί ο πάροχος πιστοποίησης να αναγνωρίσει τα στοιχεία και τις συνθήκες λειτουργίας που θα πρέπει να επιδείξει κατά τους ελέγχους, χωρίς όμως αναφέρει ποιες είναι αυτές.

1/17 θεωρεί ότι το παράρτημα ΙΙ του πδ καλύπτει τις απαιτήσεις συμμόρφωσης και είναι εξαιρετικά περιγραφικό προσδιορίζοντας το γενικό πλαίσιο των εγγράφων, στοιχείων που είναι δυνατόν να ζητηθούν στα πλαίσια ελέγχων από την αρμόδια Αρχή, ενώ, για τον περαιτέρω καθορισμό των στοιχείων συμμόρφωσης των παρόχων, παραπέμπει σε διεθνώς αναγνωρισμένα πρότυπα.

1/17 θεωρεί ότι ο πάροχος θα πρέπει να παρουσιάσει όλη τη σχετική, με τα κριτήρια του παραρτήματος ΙΙ, τεκμηρίωση όπως αυτό θα αποσαφηνισθεί από την ΕΕΤΤ βάσει των κριτηρίων που περιγράφονται αναλυτικά στους όρους του αντίστοιχου διεθνούς προγράμματος διαπίστευσης Web Trust for Certification Authorities[9], ενώ θεωρεί ότι πρέπει να υπάρχουν και άλλες προϋποθέσεις σχετικές ιδίως με την τελετή δημιουργίας του ιδιωτικού κλειδιού του παρόχου (root key generation ceremony). Παράλληλα, κατά την ίδια άποψη ο έλεγχος συμμόρφωσης πρέπει να γίνεται κατά προκαθορισμένα τακτά χρονικά διαστήματα (6 έως 12 μήνες).

1/17 αναφέρει ότι ο πάροχος υπηρεσιών πιστοποίησης, ο οποίος πρέπει να εξακριβωθεί μέσω ενός τρίτου μέρους που ακολουθεί τις προϋποθέσεις του CEN CWA 14172 :EESSI Conformity Assessment Guidance parts 1, 2 and 3, πρέπει να ακολουθεί τις προϋποθέσεις πολιτικής που ορίζονται σύμφωνα με το ETSI TS 101 456: Policy Requirements for Certification Service Providers Issuing Qualified Certificates και να χρησιμοποιεί αξιόπιστα συστήματα που ακολουθούν τις προϋποθέσεις από το CEN CWA 14167: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures, ενώ τα πιστοποιητικά πρέπει να είναι σύμφωνα με το ETSI TS 101 862: Qualified Certificate Profile.

1/17 θεωρεί ότι η συμμόρφωση με τα κριτήρια του Παραρτήματος ΙΙ αποδεικνύεται με περιοδικούς ελέγχους της Ε.Ε.Τ.Τ. στο σύστημα έκδοσης και διαχείρισης πιστοποιητικών, τόσο από την πλευρά του παρόχου, όσο από την πλευρά του χρήστη.

1/17 κάνει τις ακόλουθες διακρίσεις: Για την απόδειξη της συμμόρφωσης με τα κριτήρια (α),(β),(γ),(δ),(στ),(ζ),(θ),(ι),(ια),(ιβ) του Παραρτήματος ΙΙ προτείνεται η προσκόμιση από τον πάροχο της Πολιτικής Παροχής Υπηρεσιών Πιστοποίησης (CPS) (ή οποία για λόγους πληρότητας πρέπει να έχει δημιουργηθεί βάσει κάποιου αναγνωρισμένου προτύπου). Η συμμόρφωση με το στοιχείο (ε) διαπιστώνεται με την προσκόμιση βιογραφικών του προσωπικού, το οποίο απασχολείται σε κρίσιμες θέσεις από τον πάροχο. Για τη συμμόρφωση με το στοιχείο (η) θα πρέπει να προσκομίζονται τα κατάλληλα οικονομικά και νομικά έγγραφα του παρόχου, ενώ προτείνεται συμπληρωματικά και η προσκόμιση της πολιτικής ασφαλείας. Κατά την ίδια άποψη ο φορέας που θα οριστεί για τον έλεγχο θα πρέπει να κάνει αυτοψία του χώρου και έλεγχο υλικού και λογισμικού, ώστε να διαπιστωθεί η ευθυγράμμιση με το CPS όσον αφορά στον εξοπλισμό και τη φυσική ασφάλεια της υποδομής του παρόχου.

[9] Ο ίδιος συμμετέχων προτείνει σε περίπτωση διαπίστευση παρόχου κατά Web Trust for Certification Authorities,την αναγνώριση της ισοδυναμίας με συμμόρφωση στους όρους του Παραρτήματος ΙΙ.

1/17 θεωρεί ότι οι διαπιστευμένοι ΠΥΠ θα πρέπει να ελέγχονται ως προς τη συμμόρφωσή τους με κείμενα των Πρακτικών και των πολιτικών που τηρούν σε έγγραφο με βάση ένα σύνολο κριτηρίων πολιτικής και διαπίστευσης, προτείνοντας σχετικά το πρότυπο ETSI 101 456, ενώ ως προς τη μορφή και το περιεχόμενο των πολιτικών πιστοποίησης προτείνει ως μοντέλο τυποποίησης το RFC 2527.

1/17 προτείνει την προσκόμιση Έκθεσης Πιστοποιημένου Ελεγκτή ο οποίος θα πιστοποιεί μέσα από προκαθορισμένες διαδικασίες την συμμόρφωση του εκάστοτε παρόχου με αναφορά στα εξής: «Διεθνή πρότυπα των ψηφιακών πιστοποιητικών που εκδίδονται και αξιοπιστία των διαδικασιών παραγωγής τους, πρότυπα φυσικής ασφαλείας χώρων καθώς και διατάξεις και πλάνο για την ανάκτηση δεδομένων από φυσική καταστροφή, κατάρτιση και η εμπειρία του προσωπικού σε γνωστικό όσο και σε διοικητικό / διαδικαστικό επίπεδο, μέτρα έναντι της πλαστογράφησης πιστοποιητικών και σε περίπτωση που ο πάροχος πιστοποίησης, παράγει δεδομένα δημιουργίας υπογραφής εγγύηση τήρησης του απορρήτου, κατά τη διάρκεια της διεργασίας παραγωγής των εν λόγω δεδομένων, καθώς και διατήρηση της ιστορικότητας των δεδομένων, δημοσιευμένο ισολογισμό».

1/17 προτείνει την προσκόμιση, μεταξύ άλλων, των παρακάτω δικαιολογητικών: αποδεικτικά χρηματο-οικονομικής κατάστασης του υποψηφίου παρόχου π.χ. με την μορφή των ισολογισμών και των αποτελεσμάτων χρήσης των τελευταίων τριών (3) ετών, εγγυητική επιστολή και (ενδεχομένως) επιστολές από τράπεζες, μετοχική σύνθεση / μετοχικό κεφάλαιο, ασφαλιστήριο συμβόλαιο για αντιμετώπιση επιχειρηματικών κινδύνων, στοιχεία που να υποδηλώνουν την τεχνογνωσία και εμπειρία του ανθρώπινου δυναμικού του υποψηφίου σε σχετικά θέματα (Βιογραφικά σημειώματα από όπου θα αποδεικνύονται η εμπειρία και κατάρτιση του, Πίνακας με έργα ή δραστηριότητες ανάλογες με τις ζητούμενες υπηρεσίες), στοιχεία σχετικά με τα πρότυπα με τα οποία συμμορφώνεται το υλικό και λογισμικό που χρησιμοποιεί ο υποψήφιος (π.χ. ETSI ES 101456 - Policy for Certification Policy Requirements, ETSI TS 101862 - Qualified Certification Profile), το έγγραφο που περιγράφει την Πολιτική Ασφάλειας και Λειτουργίας (Certification Practice Statement - CPS) που θα ακολουθήσει ο υποψήφιος σε περίπτωση έγκρισης της Εθελοντικής Διαπίστευσής του από την ΕΕΤΤ. Παράλληλα επισημαίνει ότι ο σχετικός έλεγχος θα πρέπει να γίνεται από την ΕΕΤΤ τόσο κατά την υποβολή αιτήματος Εθελοντικής Διαπίστευσης όσο και σε τακτά χρονικά διαστήματα μετά την διαπίστευση (μέσω υποχρέωσης άμεσης γνωστοποίησης των όποιων αλλαγών πραγματοποιηθούν στα υποβληθέντα από τον πάροχο στοιχεία).

4. ΠΡΟΪΟΝΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ

Ορισμός Φορέων για τον Έλεγχο των Ασφαλών Διατάξεων Δημιουργίας Υπογραφής

Σύμφωνα με το ΠΔ 150/2001, ο έλεγχος της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής διενεργείται από δημόσιους ή ιδιωτικούς φορείς, που αποδεδειγμένα διαθέτουν την αξιοπιστία, ανεξαρτησία και τεχνογνωσία (συμπεριλαμβανομένης της αναγκαίας υλικοτεχνικής υποδομής), για την εκτέλεση του έργου και οι οποίοι ορίζονται από την ΕΕΤΤ.

Η ΕΕΤΤ προτίθεται να καταρτίσει κατάλογο των δημόσιων ή ιδιωτικών φορέων που θα οριστούν. Για τη διαπίστωση της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής με το Παράρτημα ΙΙΙ του ΠΔ 150/2001, κάθε ενδιαφερόμενος υποβάλλει ενώπιον της ΕΕΤΤ αίτηση, και επιλέγει από τον ως άνω κατάλογο το φορέα που θα αναλάβει την εξέταση της αίτησής του. Ο εν λόγω φορέας εισηγείται στην ΕΕΤΤ σχετικά με τη συμμόρφωση ή μη των διατάξεων δημιουργίας υπογραφής με το Παράρτημα ΙΙΙ του ΠΔ 150/2001 και η ΕΕΤΤ εκδίδει σχετική απόφαση (διαπιστωτική πράξη).

Ερώτημα 8: Πιστεύετε ότι υπάρχουν φορείς στην Ελλάδα που θα ήταν σε θέση να αναλάβουν αυτόν τον ρόλο, και, εάν ναι, ποιοι;
Με ποιο τρόπο πιστεύετε ότι θα πρέπει να διαπιστώνεται η συμμόρφωση με το Παράρτημα ΙΙΙ του ΠΔ 150/2001;

Αναφορικά με το Α' ερώτημα:
Ένα μεγάλο ποσοστό (7/17) πιστεύει ότι υπάρχουν φορείς στην Ελλάδα που θα ήταν σε θέση να αναλάβουν αυτό το ρόλο. Ως τέτοιοι φορείς περιγράφονται πανεπιστημιακά και ερευνητικά ιδρύματα (1/8), επαγγελματικά επιμελητήρια (1/8), η Deloitte & Touche (1/8) ή γενικώς αναγνωρισμένες ελεγκτικές εταιρείες (1/8), γενικότερα φορείς που ακολουθούν τις προϋποθέσεις για έναν εμπειρογνώμονα, όπως παρατίθενται στο CEN CWA 14172 EESSI Conformity Assessment Guidance part 5 (1/8), ο ΕΛΟΤ (1/8), φορείς με ικανότητα να αντεπεξέλθουν στον έλεγχο σύμφωνα με τα πρότυπα της CC και της ITSEC (1/8) καθώς και άλλοι δημόσιοι ή ιδιωτικοί φορείς με αποδεδειγμένη εμπειρία χωρίς να αναφέρονται συγκεκριμένα (3/8).

Ένας μικρός αριθμός (2/17) διαφωνεί με τον ορισμό άλλων φορέων πέραν της ΕΕΤΤ.

Τέλος, ένα μεγάλο ποσοστό (8/17) δεν τοποθετείται επί του θέματος ή δηλώνει ότι δε γνωρίζει εάν υπάρχουν σχετικοί φορείς στην Ελλάδα[10].

Αναφορικά με το Β' ερώτημα:
8 από τους 17 εξέφρασαν τις απόψεις τους ως προς το ερώτημα.
Οι προτεινόμενοι τρόποι για τη διαπίστωση της συμμόρφωσης με το Παράρτημα ΙΙΙ είναι οι εξής:

[10] 1 από τους 8 θεωρεί ότι ο ΕΛΟΤ έχει τη δυνατότητα να ορίσει τα Ελληνικά πρότυπα που θα αντιστοιχούν στα ITSEC "FIPS PUB 140-1" κλπ.

- Με κάθε πρόσφορο ή νόμιμο μέσο (1/8)
- Προσκόμιση απολύτως αναγκαίων στοιχείων από τον πάροχο (1/8)
- Πρόσβαση σε εγκαταστάσεις και στοιχεία του παρόχου (1/8)
- Τα κριτήρια που περιγράφονται αναλυτικά στους όρους του διεθνούς προγράμματος διαπίστευσης Web Trust for Certification Authorities (1/8)
- Οι κατασκευαστές συσκευών που επιθυμούν να ακολουθήσουν τις προϋποθέσεις του Παραρτήματος ΙΙΙ να υποβάλλουν αυτές τις συσκευές για διαπίστευση σε φορείς που ακολουθούν τις προϋποθέσεις που παρατίθενται στο CEN CWA 14172: EESSI Conformity Assessment Guidance part 5 και είναι αξιολογημένοι σε σχέση με τις τεχνικές προϋποθέσεις του CWA 14168: Secure Signature-Creation Devices version EAL 4. Εναλλακτικά, οι κατασκευαστές θα μπορούσαν να αυτό-αποδεικνύουν τη συμβατότητά τους στις τεχνολογικές προϋποθέσεις του CWA 14168: Secure Signature-Creation Devices version EAL 4 (2/8)
- Τα προϊόντα που η συμμόρφωσή τους με διεθνή standards ασφαλείας έχει πιστοποιηθεί από χώρα της Ε.Ε. θα πρέπει να γίνουν αποδεκτά[11]
- Αξιολόγηση και έγκριση των διατάξεων από τον ΕΛΟΤ καθώς και διαπίστωση ότι οι διατάξεις αυτές έχουν πιστοποίηση από τον αρμόδιο φορέα, ότι είναι ευθυγραμμισμένες με το επίπεδο ασφάλειας όπως αυτό θα οριστεί από την ΕΕΤΤ (πχ. FIPS 140-1 level 3 ή μεγαλύτερο ή EAL 4 ή μεγαλύτερο του, ISO 15408 Common Criteria for IT security evaluation και συμμόρφωση με το πρότυπο CWA 14170 "Security Requirements for Signature Creation Systems") (1/8)

Διαπίστωση σύμφωνα με CC και ITSEC (1/8).

<u>Προτεινόμενα Πρότυπα για τις Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής</u>

Εφόσον δημοσιευθούν στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων αριθμοί αναφοράς γενικώς αναγνωρισμένων προτύπων για προϊόντα ηλεκτρονικής υπογραφής, σύμφωνα με το άρθρο 3 παράγραφος 5 και το άρθρο 9 της Οδηγίας 99/93/ΕΚ (ΕΕ L 013 της 19/01/2000, σ. 12-20), η συμμόρφωση ενός προϊόντος ηλεκτρονικής υπογραφής με τα ανωτέρω πρότυπα αποτελεί τεκμήριο συμμόρφωσης με τις απαιτήσεις που καθορίζονται στο σημείο (στ) του Παραρτήματος ΙΙ και στο Παράρτημα ΙΙΙ του ΠΔ 150/2001.

Αναφορικά με τις ασφαλείς διατάξεις δημιουργίας υπογραφής, σε περίπτωση μη δημοσίευσης αριθμών αναφοράς γενικώς αναγνωρισμένων προτύπων, προτείνεται η συμμόρφωση με τα παρακάτω πρότυπα να θεωρείται ότι τεκμαίρει συμμόρφωση με τους όρους του Παραρτήματος ΙΙΙ του ΠΔ 150/2001.

α) CEN/ISSS WS/E-Sign "Security Requirements for Signature Creation Systems" .

[11] Προτείνεται να επιτρέπεται όμως στον τελικό χρήστη να αξιολογήσει και να επιλέξει όποια λύση θεωρεί καταλληλότερη για την περίπτωσή του

β) *Common Criteria for Information Technology security evaluation ISO/IEC 15408: Information Technology – Security Techniques- Evaluation Criteria for IT security κατ'ελάχιστον EAL 4.*

γ) *Information Technology Security Evaluation Criteria- ITSEC Evaluation κατ'ελάχιστον Ε 3*

Σε περίπτωση που τα προϊόντα χρησιμοποιούνται μέσα από ειδικά ασφαλή χώρο τότε το επίπεδο ελέγχου ασφάλειας μπορεί να είναι κατ' ελάχιστον EAL3 ή E2.

δ) *FIPS PUB 140-1 level 2 "Security Requirements For Cryptographic Modules".*

Ερώτημα 9: Συμφωνείτε με τα προτεινόμενα από την ΕΕΤΤ πρότυπα για τις ασφαλείς διατάξεις δημιουργίας υπογραφής; Έχετε να προτείνετε συμπληρωματικά άλλα πρότυπα;

5/17 δεν απάντησαν στον ερώτημα αυτό.

1/17 διαφωνεί υποστηρίζοντας σχετικά ότι πολλά από τα αναφερόμενα στην πρόταση του ερωτηματολογίου δεν αποτελούν πρότυπα και επομένως δεν είναι δυνατός ο έλεγχος βάσει αυτών, δεδομένου ότι πρότυπα εκδίδονται μόνο από τον ISO, IEC, CEN, CENELEC, ETSI και εθνικούς οργανισμούς τυποποίησης, ενώ υποστηρίζει ότι έχουν προσδιορισθεί από αυτόν τα μέχρι σήμερα υπάρχοντα πρότυπα που είναι αναγκαία για τους ελέγχους.

11/17 συμφωνούν με τα προτεινόμενα από την ΕΕΤΤ πρότυπα (κατά μία άποψη εφόσον αυτά είναι αναγνωρισμένα). Ένας από τους ανωτέρω συμμετέχοντες επισημαίνει ότι τα αναφερόμενα πρότυπα για τις «ασφαλείς διατάξεις δημιουργίας υπογραφής (α.δ.δ.υ)» πρέπει να είναι <u>ενδεικτικά</u> και να εφαρμόζονται <u>διαζευκτικώς,</u> τονίζοντας ότι σε κάθε περίπτωση θα πρέπει να παρέχεται η δυνατότητα στον Πάροχο Υπηρεσιών Πιστοποίησης να αποδείξει τη συμμόρφωση των α.δ.δ.υ που χρησιμοποιεί, με τους όρους του Παραρτήματος ΙΙΙ του ΠΔ 150/2001, με κάθε πρόσφορο ή νόμιμο μέσο. Κατά την άποψη άλλου εκ των συμμετεχόντων, θα πρέπει να παρέχεται και η δυνατότητα επιλογής του PC ως μέσου δημιουργίας ή και αποθήκευσης του key pair για όποιους χρήστες έχουν λόγους να θεωρούν ότι το PC τους είναι αρκετά ασφαλές. Άλλως, τα εν λόγω πρότυπα πρέπει να εφαρμοσθούν σε συνδυασμό με τις προϋποθέσεις του προεδρικού διατάγματος καθώς είναι τόσο ευέλικτα, ώστε μόνη η εφαρμογή των προτύπων δεν επαρκεί για την εκπλήρωση των στόχων ασφαλείας που τίθενται από αυτό, σημειώνοντας ότι η δεύτερη πρόταση του σημείου (γ) πρέπει να παραληφθεί, καθώς είναι δύσκολο να καθορισθεί εάν ο «ασφαλής χώρος» είναι πραγματικά ασφαλής και να εξασφαλισθεί ότι η α.δ.δ.υ παραμένει εντός του ασφαλούς χώρου. Μερικοί από τους ανωτέρω (4/11) προτείνουν και άλλα πρότυπα.

Συγκεκριμένα:

1/17 προτείνει πρότυπα σειράς X.500 της ITU, ενώ άλλος (1/17), προτείνει πρότυπα CWA 14168 : Secure Signature-Creation Devices version EAL 4 – Παράρτημα III, ETSI TS 101 456: Policy Requirements for Certification Service Providers Issuing Qualified Certificates – Τα περισσότερα από το Παράρτημα II, ETSI TS 101 862 : Qualified Certificate Profile - Παράρτημα I, CEN CWA 14167:Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Παράρτημα II (στ), CWA 14172: EESSI Conformity Assessment Guidance parts 1-3, Κριτήρια εμπειρογνώμονα για πάροχο υπηρεσιών πιστοποίησης, CWA 14172: EESSI Conformity Assessment Guidance part 5- , Ο εμπειρογνώμονας για τους οδηγούς δημιουργίας υπογραφής τον οποίο οι κατασκευαστές επιθυμούν να ελέγξει εάν αυτοί οι οδηγοί ακολουθούν τις προϋποθέσεις του Παραρτήματος III. ,FIPS 140-1 level 3 or Higher, CWA 14170: Security Requirements for Signature Creation Systems, Version 3,0 ή ένα αξιόπιστο σύστημα που επιβεβαιώνει επίπεδο EAL 4 ή υψηλότερο σύμφωνα με το ISO 15408 – Δημιουργία κλειδιού Αρχής Πιστοποίησης, (Certification Authority), αποθήκευση, backup and recovery συστήματα,

Άλλος (1/17) προτείνει το πρότυπο «FIPS 140-2», ενώ άλλος (1/17) από τους παραπάνω προτείνει την εξής διάκριση: Πρότυπο TS 101 456 “Policy requirements for certification authorities issuing qualified certificates” του ETSI, οι διατάξεις δημιουργίας υπογραφής (που είναι και οι διατάξεις που δημιουργείται, φυλάσσεται και δεν εγκαταλείπει ποτέ το ιδιωτικό κλειδί που δημιουργεί τις υπογραφές) για να είναι ασφαλείς πρέπει να είναι συμβατές με τις προδιαγραφές που θέτει το FIPS 140-1 level 3 ή μεγαλύτερο ή το EAL4 ή μεγαλύτερο του ISO 15408 (Common Criteria for IT security evaluation) [8], ενώ παράλληλα προδιαγράφει και τον τρόπο διαχείρισης των διατάξεων αυτών, ενώ σύμφωνα με άλλη άποψη, γίνεται η εξής διάκριση: Το FIPS 140-1 level 3 τίθεται ως όριο για την κορυφή των παρόχων (root CA) το FIPS 140-1 level 2 για τους ενδιάμεσους παρόχους στην ιεραρχία, ενώ για τις αρχές καταχώρησης (RA) θεωρείται αρκετό το FIPS 140-1 level 1. Το CPS της Globalsign αναφέρεται σε ένα ακόμα πρότυπο, το ANSI X9.66. Το CEN /ISSS WS/E-sign “Security Requirements for signature creation systems” (παραδοτέο CWA 14170) είναι ένα πρότυπο που θέτει ως ελάχιστο Evaluation Assurance Level (EAL) 4 του ISO 15408. Τα κριτήρια του αγγλικών DTI (Department of Trade and Industry) και CESG (British Governments Communications and Electronics Security Group) ονομάζονται ITSEC (UK Information Technology Security and Evaluation Criteria) και είναι αναγνωρισμένα. Όσο αφορά στη χρήση των διατάξεων σε ασφαλή χώρο, αυτό είναι αναγκαία προϋπόθεση, όπως την ορίζει το TS 101 456 “Policy requirements for certification authorities issuing qualified certificates”[4] του ETSI και το αντίστοιχο RFC 2527 “Internet X.509 PKI Certificate Policy and Certification Practices Framework” [1], ενώ η γενικότερη ασφάλεια πρέπει να είναι υλοποιημένη σύμφωνα με το ISO 17799 “Code of practice for information security management” [9]. Θεωρεί ότι το EAL3/E2 του ΕΕΤΤ, έρχεται σε αντίθεση με το EAL 4 όπως ορίζει το ETSI και το CEN/ISSS, καθώς και με όσα ορίζει η Verisign για την κορυφή της ιεραρχίας (root CA).

Προτεινόμενα Πρότυπα για την Χρήση Αξιόπιστων Συστημάτων και Προϊόντων

Αναφορικά με τη χρήση αξιόπιστων συστημάτων και προϊόντων, προτείνεται η συμμόρφωση με τα κάτωθι πρότυπα να θεωρείται ότι τεκμαίρει συμμόρφωση με το στοιχείο στ του Παραρτήματος ΙΙ του ΠΔ.150/2001

α) Common Criteria for Information Technology security evaluation ISO/IEC 15408: Information Technology – Security Techniques- Evaluation Criteria for IT security κατ'ελάχιστον EAL 4 ή,

β) Information Technology Security Evaluation Criteria- ITSEC Evaluation κατ'ελάχιστον Ε 3
Σε περίπτωση που τα προϊόντα χρησιμοποιούνται μέσα από ειδικά ασφαλή χώρο τότε το επίπεδο ελέγχου ασφάλειας μπορεί να είναι κατ'ελάχιστον EAL3 ή E2.
ή

γ) FIPS PUB 140-1 level 2 "Security Requirements For Cryptographic Modules" ή,

δ) CEN/ISSS WS/E-Sign "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures"

Αλγόριθμοι κατακερματισμού (Hash algorithms)

α) SHA-1 FIPS PUB 180-1: Secure Hash Standard ή,

β) RIPEMD ISO/IEC10118-3 : IT – Security techniques Hash-Functions Part 3: Dedicated Hash -Functions

Αλγόριθμοι υπογραφής (Signature Algorithms)

α) PKCS#1 RSA Encryption Standard ή,

β) DSA FIPS PUB 186-1: Digital Signature Standard, ή

γ) DSA variants, based on elliptic curves:
ISO/IEC 148883-3 :IT –Security Techniques- Digital signatures with appendix – Part3. ή
IEEE – Standard P1363 Section 5.3.3. ή
IEEE – Standard P1363 Section 5.3.4.

Οι ανωτέρω αλγόριθμοι κατακερματισμού και υπογραφής θεωρούνται ασφαλείς μέχρι το 2006 . Η χρονολογία αυτή δύναται να τροποποιηθεί ανάλογα με τις τεχνολογικές εξελίξεις.

Ερώτημα 10: Συμφωνείτε με τα προτεινόμενα από την ΕΕΤΤ πρότυπα για τα αξιόπιστα συστήματα και προϊόντα; Έχετε να προτείνετε συμπληρωματικά άλλα πρότυπα;

Ένα μεγάλο ποσοστό (8/17) συμφώνησε με τα πρότυπα της ΕΕΤΤ.[12]

6 από τους 17 δεν τοποθετήθηκαν επί του συγκεκριμένου ερωτήματος.

4 από τους 17 πρότειναν είτε επιπλέον πρότυπα από τα προτεινόμενα από την ΕΕΤΤ είτε διαφορετικά από αυτά. Ειδικότερα τα πρότυπα που προτάθηκαν είναι:

CWA 14168: Secure Signature-Creation Devices version EAL 4- Παράρτημα III

ETSI TS 101 456: Policy Requirements for Certification Service Providers Issuing Qualified Certificates – Τα περισσότερα από το Παράρτημα II.

ETSI TS 101 862: Qualified Certificate Profile – Παράρτημα I

CEN CWA 14167: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Παράρτημα II (στ)

CWA 14172: EESSI Conformity Assessment Guidance parts 1-3 – Κριτήρια εμπειρογνώμονα για πάροχο υπηρεσιών πιστοποίησης

CWA 14172: EESSI Conformity Assessment Guidance part 5 – Ο εμπειρογνώμονας για τους οδηγούς δημιουργίας υπογραφής τον οποίο οι κατασκευαστές επιθυμούν να ελέγξει εάν αυτοί οι οδηγοί ακολουθούν τις προϋποθέσεις του Παραρτήματος III

FIPS 140-1 level 3 or Higher, CWA 14170: Security Requirements for Signature Creation Systems, Version 3,0 ή ένα αξιόπιστο σύστημα που επιβεβαιώνει επίπεδο EAL 4 ή υψηλότερο σύμφωνα με το ISO 15408 – Δημιουργία κλειδιού Αρχής Πιστοποίησης, αποθήκευση, back up και συστήματα αποκατάστασης.

RIPEMD-160, με την επιφύλαξη ότι η υποστήριξη του εν λόγω αλγορίθμου από τους διαδεδομένους browsers παραμένει αμφισβητήσιμη.

Αλγόριθμοι κατακερματισμού (hash algorithm)

MD5
SHA-256

Tiger (192-bit)

Πρότυπα για πιστοποιητικά και πολιτικές
RFC 2527 “Internet X.509 PKI Certificate Policy and Certification Practices Framework” του IETF
RFC 2459 “Internet X.509 PKI Certificate and CRL profile” του IETF

RFC 3039 “Qualified Certificates Profile” του IETF

S 101 456 “Policy Requirements for certification authorities issuing qualified certificates” του ETSI

ANSI X9.79 “PKI practices and policy framework”

Πρότυπα Ασφάλειας

[12] 1 από τους 8 συμφώνησε με την επισήμανση ότι θα πρέπει να παρέχεται η δυνατότητα στον πάροχο να αποδείξει την αξιοπιστία των συστημάτων και των προϊόντων που χρησιμοποιεί με κάθε πρόσφορο μέσο.

Το ISO 17799 "Code of practice for information security management", είναι ένα πρότυπο ασφάλειας στο οποίο παραπέμπει και το TS 101 456 "Policy requirements for certification authorities issuing qualified certificates" του ETSI για έλεγχο της ασφάλειας των συστημάτων των παρόχων.

1 από τους 4 πρότεινε να χρησιμοποιηθούν τα πρότυπα που έχουν προσδιοριστεί μέχρι σήμερα από τον ΕΛΟΤ.

5. ΕΠΟΠΤΕΙΑ ΚΑΙ ΕΛΕΓΧΟΣ ΤΩΝ ΕΓΚΑΤΕΣΤΗΜΕΝΩΝ ΣΤΗΝ ΕΛΛΑΔΑ ΠΑΡΟΧΩΝ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ ΚΑΙ ΤΩΝ ΟΡΙΖΟΜΕΝΩΝ ΑΠΟ ΤΗΝ ΕΕΤΤ ΦΟΡΕΩΝ

Αντικείμενο και Περιεχόμενο της Εποπτείας και του Ελέγχου

Η παροχή υπηρεσιών πιστοποίησης είναι ελεύθερη και δεν υπόκειται σε προηγούμενη έγκριση. Σύμφωνα με το ΠΔ 150/2001, η ΕΕΤΤ ασκεί εποπτεία και έλεγχο επί των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών πιστοποίησης. Σε αυτά τα πλαίσια, προτείνεται όπως οι πάροχοι υπηρεσιών πιστοποίησης υποχρεώνονται σε μία απλή γνωστοποίηση της δραστηριότητάς τους και των υπηρεσιών που παρέχουν στην ΕΕΤΤ και καταχωρούνται σε ειδικό μητρώο που θα τηρεί η ΕΕΤΤ για την εφαρμογή της εποπτείας και του ελέγχου τους. Η ΕΕΤΤ, ως εποπτεύων φορέας, θα λειτουργεί κατασταλτικά σε περιπτώσεις που θα διαπιστώνεται αυτεπάγγελτα ή μετά από καταγγελία παράβαση των διατάξεων της κείμενης νομοθεσίας.

Ερώτημα 11: Συμφωνείτε με αυτή την μορφή υλοποίησης του ελέγχου και της εποπτείας; Πιστεύετε ότι πρέπει να είναι πιο αυστηρή;

3/17 δεν απάντησαν στο ερώτημα αυτό.

8/17 συμφωνούν με την προτεινόμενη μορφή υλοποίησης του ελέγχου και της εποπτείας. Ένας από αυτούς προτείνει την πρόβλεψη στο πειθαρχικό μέρος του Κανονισμού της ΕΕΤΤ, κυρώσεων για τους παρόχους που παραλείπουν να γνωστοποιήσουν τη δραστηριότητά τους στην ΕΕΤΤ («nulla poena sine lege»), προκειμένου η νομοθετική επιταγή για γνωστοποίηση να μην αποτελεί lex imperfecta. Ως κυρώσεις προτείνει το πρόστιμο, ανάκληση της διαπίστευσής του, ενώ θεωρεί ως οριακό ζήτημα την δυνατότητα (ακούσιας ιδίως) διαγραφής του παρόχου από το μητρώο[13]. Τονίζεται πάντως ότι οι προβλεπόμενες κυρώσεις δεν πρέπει να φτάνουν μέχρι την απαγόρευση της παροχής υπηρεσιών πιστοποίησης εκ μέρους του μη (αυτο)γνωστοποιουμένου παρόχου.

Κατά άλλη άποψη (2/17) επισημαίνεται η ανάγκη συνεχούς, περιοδικού ή έκτακτου ελέγχου των παρόχων (κατά την μία άποψη επιβάλλεται διενέργεια προληπτικών περιοδικών ελέγχων από την ΕΕΤΤ, για συγκεκριμένους λόγους εκ των προτέρων προβλεπόμενους), ενώ τονίζεται ότι σε περίπτωση που ως αποτέλεσμα του ανωτέρω ελέγχου διαπιστώνονται παραβάσεις στις διατάξεις του πδ 150/2001, πέρα από την επιβολή των πρόστιμων που προβλέπονται στο πδ, θα πρέπει να δημοσιοποιείται η παράβαση στους χρήστες των υπηρεσιών του παρόχου. Κατά την μία από τις δύο απόψεις στην περίπτωση των Πάροχων Υπηρεσιών Πιστοποίησης που εκδίδουν και Αναγνωρισμένα Πιστοποιητικά θα πρέπει να εξασφαλισθεί από την ΕΕΤΤ ότι είναι σαφής η διαφοροποίηση ανάμεσα στους Πάροχους που εκδίδουν αναγνωρισμένα πιστοποιητικά και σε εκείνους που ΔΕΝ εκδίδουν αναγνωρισμένα πιστοποιητικά.

[13] Ο ίδιος συμμετέχων επισημαίνει ότι στην περίπτωση αυτή το μητρώο θα έτεινε να λειτουργεί ως παράλληλος θεσμός διαπίστευσης με προϋποθέσεις λιγότερες από τις νόμιμες.

Σύμφωνα με άλλη άποψη θα πρέπει να προβλεφθεί διαδικασία προηγούμενης ακρόασης των ενδιαφερομένων καθώς και ένας μηχανισμός συμβιβαστικής επίλυσης διαφορών που μπορούν να προκύψουν (π.χ σε περίπτωση που διαπιστωθούν ή γίνει επίκληση ελαττωμάτων του πιστοποιητικού που κάθε φορά εκδίδεται, κ.ά.).

Άλλος συμφωνεί, υπό την προϋπόθεση ότι υπάρχει ενημέρωση των χρηστών για τη χορήγηση κρατικής έγκρισης σε κάποιους παρόχους υπηρεσιών πιστοποίησης, προτείνοντας σχετικά τη δημιουργία ελεύθερα προσβάσιμου καταλόγου με τους παρόχους που έχουν την έγκριση της ΕΕΤΤ (εθελοντικά διαπιστευμένους) και εκείνους τους παρόχους που δεν την έχουν, καθώς και γνωστοποίηση ύπαρξης του καταλόγου σε όλους τους πολίτες. Κατά την ίδια άποψη η έγκριση από την ΕΕΤΤ είναι επιβεβλημένη σε περίπτωση έκδοσης αναγνωρισμένων πιστοποιητικών, σε συμμόρφωση με την οδηγία της ΕΚ.

1/17 θεωρεί ότι αρκεί η άσκηση εποπτείας επί των παρόχων υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά, ενώ κατά άλλη άποψη (1/17) τουλάχιστον στην αρχή θα πρέπει η Ε.Ε.Τ.Τ. να λειτουργεί και προληπτικά συμμετέχοντας στη διαδικασία διαπίστευσης, ενώ ο έλεγχος θα πρέπει να είναι όσον το δυνατόν αυστηρότερος, εστιαζόμενος περισσότερο στις διαδικασίες και λιγότερο στο υλικό.

Άλλος εκ των συμμετεχόντων θεωρεί ότι δεν πρέπει να είναι αναγκαία η γνωστοποίηση της έναρξης παροχής υπηρεσιών για πιστοποιητικά που εκδίδονται για γενικούς σκοπούς (σε μη αναγνωρισμένο επίπεδο), δεδομένου ότι τέτοιου είδους πιστοποιητικά είναι διαθέσιμα on line, και θα μπορούσε να δημιουργηθεί σύγχυση μεταξύ προσφοράς υπηρεσιών από την Ελλάδα και προσφοράς υπηρεσιών στην Ελλάδα.

2/17 διαφωνούν. Συγκεκριμένα, ο ένας από αυτούς πιστεύει ότι η απλή γνωστοποίηση είναι ανεπαρκής θεωρώντας ότι, εφόσον επέρχονται οι συνέπειες του άρθρου 3.1 του πδ, θα πρέπει, για λόγους διασφάλισης της ασφάλειας των συναλλαγών και προστασίας του καταναλωτή, να ενταχθεί η πιστοποίηση στο προληπτικά ελεγχόμενο (ως προς τη νομιμότητα) σύστημα της εθελοντικής διαπίστευσης[14]. Κατά τον άλλο διαφωνούντα, η ΕΕΤΤ, υπό τη σημερινή μορφή της, δεν έχει καμία σχέση με συστήματα εθελοντικής ή μη διαπίστευσης ούτε μπορεί να ελέγχει κανένα τέτοιο φορέα[15].

[14] Ο ίδιος συμμετέχων παραπέμπει σε περίπτωση αμφιβολίας περί εξουσιοδότησης της ΕΕΤΤ, στο άρθρο 4.8 του πδ 150/2001.

[15] Κατά την άποψη αυτή, ο ρόλος της ΕΕΤΤ περιοριζεται στο να αποτελεί:
την κορυφή του συστήματος πιστοποίησης,
τον εκπρόσωπο της Ελλάδας στις διαδικασίες αμοιβαίας αναγνώρισης και στην επιτροπή του άρθρου 9,
το εργαλείο του κράτους-μέλους για την ικανοποίηση των υποχρεώσεών του που απορρέουν από την Οδηγία 99/93, και δύναται να χρησιμοποιεί τα κατάλληλα μέσα (π.χ. ΕΛΟΤ) για την εκτέλεση των σκοπών της.

Επιπλέον, η ΕΕΤΤ ασκεί εποπτεία και έλεγχο επί των φορέων διαπίστευσης και ελέγχου της συμμόρφωσης των υπογραφών προς το Παράρτημα ΙΙΙ του ΠΔ150/2001.

Ερώτημα 12: Ποια μορφή πιστεύετε ότι θα πρέπει να έχει η εποπτεία και ο έλεγχος των φορέων αυτών;

Η πλειοψηφία των συμμετεχόντων (11/17) συμφωνεί με την άσκηση εποπτείας και ελέγχου απο την ΕΕΤΤ.

Ένα ποσοστό (4/17) δεν τοποθετείται επί του συγκεκριμένου ερωτήματος.

1 από τους 17 θεωρεί ότι ο έλεγχος της ΕΕΤΤ δεν είναι αναγκαίος εφόσον επιλεχθεί η ακόλουθη λύση: οι φορείς θα πρέπει να έχουν δικαίωμα έκδοσης πιστοποιητικού για τη συμμόρφωση μίας διάταξης με το επίπεδο ασφάλειας κάποιου προτύπου (πχ FIPS 140-1 level 3 ή EAL4 του ISO 15408 Common Criteria for IT security evaluation). Αν οι φορείς είναι εγκεκριμένοι από τον αρμόδιο φορέα (πχ. ISO ή ΕΛΟΤ κλπ) στο να εκδίδουν πιστοποιητικά συμμόρφωσης τότε δε χρειάζεται περαιτέρω έλεγχος (ο φορέας συνήθως πρέπει να ακολουθεί κάποια συγκεκριμένη μεθοδολογία ελέγχου συμμόρφωσης με το πρότυπο (πχ. χρήση λογισμικού CCTOOL για τον υπολογισμό του EAL της διάταξης ISO 17799, standard security policies/CPSs, sufficient audit mechanisms).

1 από τους 17 διαφωνεί με την άσκηση εποπτείας και ελέγχου από την ΕΕΤΤ.

Ειδικότερα, προτείνονται οι ακόλουθοι τρόποι άσκησης εποπτείας και ελέγχου από την ΕΕΤΤ:

- Με τα έννομα μέσα του διοικητικού δικαίου (1/11)
- Με όρους που θα περιλαμβάνονται στη σύμβαση ανάθεσης των καθηκόντων από την ΕΕΤΤ στους φορείς (1/11)
- Θέσπιση προτύπων ποιότητας από ΕΕΤΤ (2/11)
- Διαδικασία από-διαπίστευσης σε περιπτώσεις που αυτό επιβάλλεται λόγω παραβίασης προϋποθέσεων (1/11)
- Περιοδικοί έλεγχοι από ΕΕΤΤ (4/11)
- Αίτηση παροχής πληροφοριών και στοιχείων (1/11)
- Έλεγχος σύμφωνα με τα πρότυπα EN45001/11/12 και ISO17025

6. ΣΥΣΤΑΣΕΙΣ ΓΙΑ ΑΣΦΑΛΗ ΕΠΑΛΗΘΕΥΣΗ ΤΗΣ ΥΠΟΓΡΑΦΗΣ

Το ΠΔ 150/2001 στο Παράρτημα IV περιλαμβάνει συστάσεις για την ασφαλή επαλήθευση της υπογραφής.

Ερώτημα 13: Κρίνεται αναγκαία την τήρηση του εν λόγω παραρτήματος; Με ποιόν τρόπο θεωρείτε ότι διασφαλίζετε η εφαρμογή του;

7/17 δεν απάντησαν στο ερώτημα.

5/17 απάντησαν θετικά.

Ο ένας από αυτούς θεωρεί ότι χρήζει περαιτέρω διευκρίνησης η φράση "διασφαλίζεται με εύλογη βεβαιότητα", ενώ κατά άλλη άποψη ο σκοπός που εξυπηρετεί καλύπτεται και από την εφαρμογή των αναγνωρισμένων προτύπων.

Κατά άλλη άποψη η τήρηση του Παραρτήματος είναι αναγκαία αφού όμως καθοριστεί ο τρόπος υλοποίησης του η δε εφαρμογή του διασφαλίζεται με την ένταξη του ελέγχου του στο σύνολο των περιοδικών ελέγχων που θα διασφαλίζουν τη συνέχεια της διαπίστευσης.

Κατά άλλη άποψη, η τήρηση του παραρτήματος VI επιβάλλεται για λόγους προστασίας του χρήστη ο οποίος λαμβάνει το πιστοποιητικό και είναι εκτεθειμένος σε κινδύνους εξαπάτησης. Κατά την ίδια πάντα άποψη η εφαρμογή του παραρτήματος με δεδομένο λογισμικό, παραπέμπει σε σωστή ενημέρωση του χρήστη για τις διαδικασίες που πρέπει να τηρήσει και τους κινδύνους που επιφυλάσσει η παράβλεψή τους. Η χρήση αναγνωρισμένου λογισμικού μπορεί να διασφαλίσει εν μέρει την εφαρμογή του παραρτήματος, καθώς το μεγαλύτερο τμήμα των προδιαγραφών που θέτει, ικανοποιείται αυτόματα από αυτό. Ο συνδυασμός των παραπάνω είναι αποτελεσματικός. Επιπροσθέτως, αναγνωρίζοντας τις δυσκολίες, επισημαίνει την αναγκαιότητα επιβεβαίωσης της ηλεκτρονικής υπογραφής και πέρα από την περίοδο εγκυρότητος του ζεύγους κλειδιών που χρησιμοποιήθηκαν για την δημιουργία της, παραπέμποντας για τους σχετικούς μηχανισμούς οι οποίοι άπτονται της χρονικά συσχετισμένης μη-άρνησης (time related non-repudiation) στο TS 101 733 "Electronic Signature Formats" [6].

1/17 θεωρεί ότι το παράρτημα είναι χρήσιμο σαν σύσταση αλλά δεν γνωρίζει με ποιο τρόπο θα μπορούσε να διασφαλιστεί η εφαρμογή του.

Κατά άλλη άποψη (1/17) το παράρτημα πρέπει να έχει τη μορφή συστάσεων και όχι προϋποθέσεων, ενώ, σε περίπτωση εφαρμογής του, προτείνεται ως κατευθυντήρια οδηγία η εφαρμογή των διαδικασιών που προβλέπει το CWA 14171 Procedures for Electronic Signature Verification V 1.0.5.

1/17 υποστηρίζει ότι οι διαπιστευμένοι ΠΥΠ πρέπει να συστήσουν εγκεκριμένες διατάξεις δημιουργίας και επαλήθευσης υπογραφής στους πελάτες τους προκειμένου να τους συνδράμουν στην χρήση ασφαλών διατάξεων, σημειώνοντας ότι οι εν λόγω διατάξεις θα πρέπει συγχρόνως να εκτιμηθούν σύμφωνα με το CC/ITSEC λαμβάνοντας υπόψη τους στόχους ασφαλείας του διατάγματος.

1/17 θεωρεί ότι πρόκειται κατά βάση για πολιτικό ζήτημα, η απάντηση στο οποίο μπορεί να δοθεί μόνο με βάση εκτιμήσεις για τις οποίες αρμοδιότητα έχει μόνον η ίδια ΕΕΤΤ, αλλά και –γενικότερα- τα αρμόδια όργανα πολιτικού σχεδιασμού της χώρας στον τομέα της επιχειρηματικής ανάπτυξης και των τηλεπικοινωνιών. Συγκεκριμένα, κατά την άποψη αυτή, η σύσταση του παραρτήματος IV αναφέρεται στο custom-made λογισμικό που πιθανώς να αναπτύσσεται από Π.Υ.Π. ή προμηθευτές τους για την διενέργεια των διαδικασιών υπογραφής και επαλήθευσης μιας υπογραφής. Θα πρέπει να εξεταστεί από την ΕΕΤΤ εάν θα 'διαπιστεύει' τέτοια προϊόντα (λογισμικό για την δημιουργία ηλεκτρονικής υπογραφής και την επαλήθευση ηλεκτρονικών υπογραφών και πιστοποιητικών) τόσο ως προς την συμμόρφωσή τους προς το παράρτημα ΙΙΙ (όσον αφορά την δημιουργία της υπογραφής) αλλά και ως προς το παράρτημα IV (όσον αφορά τον τρόπο επαλήθευσης μιας υπογραφής), ενώ παράλληλα θα πρέπει η ΕΕΤΤ να χαράξει ιδιαίτερες προδιαγραφές για αυτά τα 'προγράμματα' που θα εξασφαλίζουν ή τουλάχιστον θα προδιαθέτουν σε μία συμβατότητα μεταξύ των παρεχόμενων (σε εθνικό και ευρωπαϊκό επίπεδο) πιστοποιητικών (όπως π.χ. να αναγνωρίζουν τις πολιτικές των πιστοποιητικών που επαληθεύουν από τον αριθμό OID που θα αναφέρεται στο extended πεδίο 'Certificate Policies' του πιστοποιητικού)[16].

1/17 διαφωνεί θεωρώντας ότι δεν είναι σκόπιμη η τήρηση του Παραρτήματος IV, διότι η διασφάλιση των προτεινόμενων αναγκών καλύπτεται μέσω της χρησιμοποιούμενης τεχνολογίας. Κατά την ίδια άποψη, οι απαιτήσεις που περιγράφονται στο Παράρτημα IV υλοποιούνται με χρήση εξελιγμένων αλγορίθμων και μηχανισμών κρυπτογράφησης οι οποίοι αποτελούν ιδιοκτησία του κατασκευαστή. Σε περίπτωση αλλαγής των αρχικών δεδομένων ο μηχανισμός έχει την ικανότητα να ειδοποιήσει αυτόματα τον χρήστη.

[16] Κατά την ίδια άποψη το γεγονός ότι το παράρτημα IV διατυπώνεται ως Σύσταση (χωρίς νομικά δεσμευτική ισχύ), οφείλεται στο δισταγμό του κοινοτικού νομοθέτη να υποχρεώσει τα κράτη μέλη να αναγκάσουν τους παρόχους υπηρεσιών πιστοποίησης σε προμήθεια προκαθορισμένων προϊόντων ηλεκτρονικής υπογραφής, δεδομένου ότι η Ευρωπαϊκή Ένωση επιδιώκει να παραμείνει κατά το δυνατόν αμερόληπτη και ουδέτερη ανάμεσα στις διάφορες τεχνολογίες ηλεκτρονικής υπογραφής, λαμβάνοντας υπόψη το εύλογο συμφέρον κάποιων χωρών να προωθήσουν εμπορικά την τεχνολογία τους σε βάρος των υπολοίπων.

7. ΠΑΡΑΡΤΗΜΑ Ι

ΦΟΡΕΙΣ ΠΟΥ ΑΠΑΝΤΗΣΑΝ

1. ΑΣΥΚ Α.Ε.
2. ΕΒΕΑ
3. ΕΛΟΤ
4. ΕΡΓΑΣΤΗΡΙΟ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΤΜΗΜΑΤΟΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΑΘΗΝΩΝ
5. ΚΑΡΑΓΙΩΡΓΙΟΥ Ι. & ΣΥΝΕΡΓΑΤΕΣ
6. ΛΑΝ-ΝΕΤ ΕΠΙΚΟΙΝΩΝΙΕΣ Α.Ε.
7. ΟΤΕΝΕΤ
8. ΣΙΟΥΛΗΣ ΧΡΗΣΤΟΣ
9. ADACOM A.E
10. DELOITTE & TOUCHE
11. ENCODE A.E.
12. EUROBANK
13. EXPERTNET A.E.
14. GLOBAL SIGN
15. SPACE HELLAS
16. STET HELLAS A.E.B.E
17. TUVIT