Πρόσκληση υποβολής απόψεων σχετικά με τις Ηλεκτρονικές Υπογραφές σε θέματα που άπτονται της Παροχής Υπηρεσιών Πιστοποίησης και της Εθελοντικής Διαπίστευσης.

ΣΗΜΕΙΩΣΗ

Το παρόν κείμενο καταρτίστηκε από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων και αφορά το κανονιστικό πλαίσιο σχετικά με την παροχή υπηρεσιών πιστοποίησης και την εθελοντική διαπίστευση.

Η ΕΕΤΤ προσκαλεί τους ενδιαφερόμενους φορείς να παρουσιάσουν τις απόψεις τους απαντώντας στις ερωτήσεις του κειμένου, δηλώνοντας ευκρινώς τον αριθμό του ερωτήματος στο οποίο αναφέρεται η κάθε απάντηση. Οι απαντήσεις θα πρέπει να είναι περιεκτικές, σαφείς, και οι όποιες απόψεις να παρατίθονται με σχετική τεκμηρίωση. Οι ενδιαφερόμενοι δεν είναι υποχρεωμένοι να απαντήσουν σε όλες τις ερωτήσεις.

Η ΕΕΤΤ δεν δεσμεύεται από τα αποτελέσματα της παρούσας διαδικασίας υποβολής απόψεων ως προς τις ρυθμίσεις που θα υιοθετήσει.

Τυχόν ανώνυμες απαντήσεις δεν θα ληφθούν υπόψη. Οι απαντήσεις θα πρέπει να φέρουν την ένδειξη: «Υποβολή απόψεων σε θέματα που άπτονται της παροχή υπηρεσιών πιστοποίησης και της εθελοντικής διαπίστευσης.».

Οι απαντήσεις θα πρέπει να υποβληθούν επώνυμα, στην Ελληνική γλώσσα, σε έντυπη και ηλεκτρονική μορφή μέχρι την Παρασκευή 30 Νοεμβρίου 2001 στις παρακάτω διευθύνσεις :

Ταχυδρομική διεύθυνση:

Για την «Υποβολή απόψεων σε θέματα που άπτονται της παροχή υπηρεσιών πιστοποίησης και της εθελοντικής διαπίστευσης.».
Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
Λεωφόρος Κηφισίας 60
151 25 Μαρούσι

Ηλεκτρονική διεύθυνση:

esign@eett.gr

Πρόσκληση υποβολής απόψεων σε θέματα σχετικά με τις Ηλεκτρονικές Υπογραφές σε θέματα που άπτονται της παροχή υπηρεσιών πιστοποίησης και της εθελοντικής διαπίστευσης.

ΕΙΣΑΓΩΓΗ

Με το ΠΔ 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές» (ΦΕΚ 125/Α/2001) έγινε η προσαρμογή της Ελληνικής νομοθεσίας προς τις διατάξεις της Οδηγίας 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 «Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές» (EEL 13/19.1.2000).

Η ΕΕΤΤ στα πλαίσια των αρμοδιοτήτων της που απορρέουν από το ΠΔ 150/2001 προτίθεται να εκδώσει Κανονισμό ο οποίος θα ρυθμίζει:

- τη διαδικασία, τους όρους και τις προϋποθέσεις της εθελοντικής διαπίστευσης των παρόχων υπηρεσιών πιστοποίησης
- τη διαπίστωση της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής προς το Παράρτημα ΙΙΙ του ΠΔ 150/2001
- την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών πιστοποίησης και των από την ΕΕΤΤ οριζόμενων φορέων για τη διαπίστωση της συμμόρφωσης των ασφαλών διατάξεων δημιουργίας υπογραφής προς το παράρτημα ΙΙΙ του ΠΔ 150/2001.

Η ΕΕΤΤ ενόψει της έκδοσης του Κανονισμού, προκειμένου να ανταποκριθεί όσο το δυνατόν πιο αποτελεσματικά στις απαιτήσεις που δημιουργούνται στην Ελλάδα από την ανάπτυξη της αγοράς των υπηρεσιών πιστοποίησης, θέτει σε δημόσια διαβούλευση συγκεκριμένα ζητήματα, για τα οποία θεωρεί ότι η άποψη και εμπειρία της αγοράς θα είναι ιδιαίτερα εποικοδομητική.

Ι. 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;

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;

II. 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;

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 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;

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;

<u>Έκδοση Αναγνωρισμένων Πιστοποιητικών Μόνο σε Περιβάλλον Ασφαλών Διατάξεων Δημιουργίας Υπογραφής</u>

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;

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;

ΙΙΙ. 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;

Προτεινόμενα Πρότυπα για τις Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής

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" .*

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;

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 Ε2.
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;

IV. 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;

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;

V. ΣΥΣΤΑΣΕΙΣ ΓΙΑ ΑΣΦΑΛΗ ΕΠΑΛΗΘΕΥΣΗ ΤΗΣ ΥΠΟΓΡΑΦΗΣ

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

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