ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΟΙΚΟΝΟΜΙΑΣ & ΟΙΚΟΝΟΜΙΚΩΝ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΦΟΡΟΛΟΓΙΑΣ
ΔΙΕΥΘΥΝΣΗ ΚΩΔΙΚΑ ΒΙΒΛΙΩΝ & ΣΤΟΙΧΕΙΩΝ
ΤΜΗΜΑ ΦΟΡΟΛΟΓΙΚΩΝ ΤΑΜΕΙΑΚΩΝ ΜΗΧΑΝΩΝ & ΣΥΣΤΗΜΑΤΩΝ

ΠΟΡΙΣΜΑ

ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΟΙΚΟΝΟΜΙΚΩΝ ΠΟΥ ΣΥΣΤΗΘΗΚΕ ΜΕ ΤΗΝ ΑΥΟ 1047819/815/Α0006 (ΦΕΚ 732 Β'/13-06-2002), ΓΙΑ ΤΗ ΣΥΓΓΡΑΦΗ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ ΑΣΦΑΛΩΝ ΦΟΡΟΛΟΓΙΚΩΝ ΜΗΧΑΝΙΣΜΩΝ ΣΗΜΑΝΣΗΣ ΤΩΝ ΕΚΔΙΔΟΜΕΝΩΝ ΑΠΟ ΑΥΤΟΥΣ ΣΤΟΙΧΕΙΩΝ ΚΑΙ ΤΗ ΜΕΛΕΤΗ ΤΡΟΠΟΠΟΙΗΣΗΣ ΤΩΝ ΣΧΕΤΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΤΟΥ Ν. 1809/1988 ΚΑΙ ΤΗΣ ΚΑΤΑΡΓΗΣΗΣ ΤΗΣ ΔΙΑΤΡΗΣΗΣ ΤΩΝ ΣΤΟΙΧΕΙΩΝ ΤΟΥ Κ.Β.Σ..

ΙΟΥΝΙΟΣ - ΑΥΓΟΥΣΤΟΣ 2002

Πρόταση Ασφαλούς Τρόπου Σήμανσης Μηχανογραφικά Εκδιδομένων Στοιχείων

Περιεχόμενα

9. Βιβλιάριο Συντήρησης και Επισκευών

10. Έγκριση και χορήγηση άδειας καταλληλότητας

10.1. Διαδικασία
10.2. Δικαιολογητικά
10.3. Δείγμα Ελέγχου
10.4. Διάθεση Εξοπλισμού και Λογισμικού Ελέγχου

11. Παρακολούθηση ΕΑΦΔΣΣ μέσω του συστήματος TAXIS.

Παράρτημα Π1- Ασφαλής Hash Αλγόριθμος SHA-1

Π1. Εισαγωγική Περιγραφή
Π1.1. Γενικά για τους Ασφαλείς Αλγόριθμους SHA
Π1.2. Ορισμοί
Π1.2.1 Λεξιλόγιο των χρησιμοποιούμενων όρων και ακρωνυμίων
Π1.2.2 Αλγοριθμικές Παράμετροι, Χρησιμοποιούμενα Σύμβολα, και Όροι
Π1.2.2.1 Παράμετροι
Π1.2.2.2 Σύμβολα πράξεων
Π1.3. Συμβολισμοί και Κανόνες Παράστασης
Π1.3.1 Αλληλουχίες (σειρές) από Bit και Ακέραιοι.
Π1.3.2 Πράξεις επί των Λέξεων.
Π1.4. Συναρτήσεις και Σταθερές
Π1.4.1 Συναρτήσεις που χρησιμοποιούνται στον αλγόριθμο SHA-1.
Π1.4.2 Σταθερές που χρησιμοποιούνται στον αλγόριθμο SHA-1.
Π1.5. Προεπεξεργασία
Π1.5.1 Συμπληρώνοντας το μήνυμα («γέμισμα» του μηνύματος).
Π1.5.1.1 SHA-1 *(και SHA-256)*
Π1.5.2 Ανάλυση (τμηματοποίηση) του «γεμισμένου» μηνύματος
Π1.5.2.1 SHA-1 *(και SHA-256)*
Π1.5.3 Ορισμός και απόδοση Αρχικής Hash Τιμής ($H^{(0)}$)
Π1.5.3.1 SHA-1
Π1.6. Ασφαλείς HASH Αλγόριθμοι.
Π1.6.1 SHA-1
Π1.6.1.1 SHA-1 Προ-επεξεργασία
Π1.6.1.2 SHA-1 Υπολογισμός Hash
Π1.6.1.3 Εναλλακτική μέθοδος υπολογισμού του αλγορίθμου SHA-1 για τη σύνοψη (υπογραφή) ενός μηνύματος.
Π1.Α. Παράρτημα Α : Παραδείγματα SHA-1.
Π1.Α.1 SHA-1 Παράδειγμα Μηνύματος ενός μόνον τμήματος (1-block message)
Π1.Α.2 SHA-1 Παράδειγμα Μηνύματος πολλαπλών τμημάτων (Multi-block message)
Π1.Α.3 SHA-1 Αναφορά αποτελέσματος σε παράδειγμα Μηνύματος μεγάλου Μήκους

Παράρτημα Π2- ΠΡΟΤΕΙΝΟΜΕΝΟΣ Πίνακας Ελληνικών ASCII – ΕΛΟΤ 928

Πρόταση Ασφαλούς Τρόπου Σήμανσης Μηχανογραφικά Εκδιδομένων Στοιχείων

1. Γενικά

1.1. Υπάρχουσα κατάσταση

1.1.1. Η θεώρηση / διάτρηση των στοιχείων που επιβάλουν οι διατάξεις του Κ.Β.Σ. αποτελεί μέχρι τώρα τη βασική ασφαλιστική δικλείδα αποτροπής φορολογικών καταστρατηγήσεων (με τη μέθοδο της αντικατάστασης αυτών με εικονικά – πλαστά στοιχεία και την εμφάνιση διαφοροποιημένων φορολογικών δεδομένων). Η θεώρηση / διάτρηση λοιπόν που επιβάλλεται μέχρι τώρα από τον Κ.Β.Σ. είναι στην ουσία μια προσέγγιση σήμανσης και αυθεντικοποίησης των στοιχείων.
1.1.2. Με την διάτρηση δεν «σημαίνονται» τα ίδια τα στοιχεία και δεδομένα που αναγράφονται στα εκδιδόμενα δελτία, αλλά μόνον το μέσον, ο φορέας (δηλ. το χαρτί) στο οποίο αυτά εκτυπώνονται.
1.1.3. Η διαδικασία αυτή, εκτός του ότι δεν αποτρέπει ολοκληρωτικά την κυκλοφορία εικονικών στοιχείων, στις περισσότερες περιπτώσεις, – και κυρίως λόγω του όγκου των προς θεώρηση / διάτρηση στοιχείων –, αυξάνει σημαντικά το λειτουργικό κόστος τόσο για τις φορολογικές υπηρεσίες όσο και για τις επιχειρήσεις – επιτηδευματίες που είναι υπόχρεοι εφαρμογής του μέτρου αυτού.

1.2. Σκοπός

1.2.1 Σκοπός του προτεινόμενου μέτρου είναι, η σχετική βελτίωση της αξιοπιστίας της σήμανσης των εκδιδομένων από τις επιχειρήσεις φορολογικών στοιχείων, η βελτίωση των διαδικασιών ελέγχου και η μείωση του κόστους μέσω της αποσυμφόρησης των εργασιών της σήμανσης και της ελαχιστοποίησης του απαραίτητου αποθηκευτικού χώρου διαφύλαξης στοιχείων.
1.2.2. Ειδικά με τα προτεινόμενα μέτρα επιτυγχάνεται :

- η σήμανση και η ασφαλής πιστοποίηση της γνησιότητας των εκδιδομένων στοιχείων,
- η δυνατότητα ελέγχου – επαλήθευσης της γνησιότητας των εκδοθέντων και αποθηκευθέντων στοιχείων
- η διευκόλυνση του ελεγκτικού μηχανισμού της διασταύρωσης των στοιχείων
- η ανεξαρτητοποίηση της διαδικασίας της σήμανσης από τον εκδότη των στοιχείων, από τις φορολογικές υπηρεσίες
- η μείωση του φόρτου εργασίας των φορολογικών υπηρεσιών
- η σημαντική μείωση του λειτουργικού κόστους της διαδικασίας σήμανσης των στοιχείων

1.2.3. Με το προτεινόμενο μέτρο επηρεάζεται ελάχιστα ο τρόπος έκδοσης στοιχείων, στις επιχειρήσεις και τους επιτηδευματίες που εκδίδουν μηχανογραφικά μέσω Η/Υ τα στοιχεία τους, ενώ το περιβάλλον εργασίας δεν μεταβάλλεται καθόλου.
Επίσης με την καθιέρωση του μέτρου αυτού, υιοθετείται ουσιαστικά, ένας γενικός, σύγχρονος και ασφαλής τρόπος διαφύλαξης των αντιγράφων των εκδιδομένων στοιχείων σε ηλεκτρονική μορφή. Το αποτέλεσμα αυτού θα είναι η σημαντική εξοικονόμηση αποθηκευτικού χώρου φύλαξης στοιχείων, και η απελευθέρωση σημαντικών πόρων που διατίθενται για το σκοπό αυτό. Συγχρόνως καθίσταται ευκολότερος και ταχύτερος ο έλεγχος και η επαλήθευση των στοιχείων αυτών.

1.3. Συνοπτική περιγραφή απαραίτητου εξοπλισμού με τον προτεινόμενο τρόπο.

1.3.1. Ο εκδότης του στοιχείου (πχ Τιμολογίου, Δελτίου Αποστολής, Τιμολογίου – Δελτίου Αποστολής κλπ), θα πρέπει να διαθέτει :

- Ειδικό φορολογικό μηχανισμό (ασφαλή διάταξη) σήμανσης στοιχείων
- Η/Υ με κατάλληλο λογισμικό υποστήριξης και δυνατότητες επικοινωνίας με τον ειδικό φορολογικό μηχανισμό σήμανσης.

Σημ.
Μια πρώτη προσέγγιση κόστους απόκτησης του σχετικού εξοπλισμού και της προσαρμογής του λογισμικού εκτιμάται από 600€ έως 700€, αλλά θα πρέπει να επισημανθεί ότι με το ν.1809/1988 προβλέπεται η έκπτωση και η απόσβεση της δαπάνης αυτής από τις επιχειρήσεις και τους επιτηδευματίες που θα υποχρεωθούν στη χρήση του μέτρου.
Αποσύρεται από την αρχική πρόταση εφαρμογής του μέτρου, η σχετική παράγραφος για τις απαιτήσεις λογισμικού του Η/Υ του αποδέκτη των στοιχείων, περί υποδοχής, ελέγχου και καταχώρησης του κωδικού σήμανσης, λόγω του χρόνου – κόστους καταχώρησης.

1.4. Συνοπτική περιγραφή διαδικασίας έκδοσης στοιχείων με τον προτεινόμενο τρόπο.

1.4.1. Η εκτύπωση – έκδοση των στοιχείων εξακολουθεί να γίνεται από τον εκτυπωτικό μηχανισμό του εκδότη, όπως και πριν την εφαρμογή του μέτρου.
1.4.2. Μετά την καταχώρηση και τη διαμόρφωση των προς εκτύπωση δεδομένων στον Η/Υ και την ενεργοποίηση της διαδικασίας έκδοσης – εκτύπωσης του στοιχείου, το λογισμικό του Η/Υ επικοινωνεί και αποστέλλει στον ειδικό φορολογικό μηχανισμό σήμανσης, το σύνολο των δεδομένων του υπό έκδοση στοιχείου.
1.4.3. Ο ειδικός φορολογικός μηχανισμός σήμανσης, δέχεται τα δεδομένα αυτά, τα επεξεργάζεται με ειδικό ασφαλή αλγόριθμο δημιουργίας σύνοψης – υπογραφής και επιστρέφει πίσω στον διασυνδεόμενο Η/Υ, το αποτέλεσμα αυτής της επεξεργασίας, δηλ. έναν κωδικό, μια αλληλουχία χαρακτήρων που αποτελεί μοναδικό ηλεκτρονικό αποτύπωμα των δεδομένων του υπό έκδοση στοιχείου, αποθηκεύει τον κωδικό αυτό σε μνήμη εργασίας που διαθέτει για το σκοπό αυτό και εκδίδει σχετικό δελτίο – απόδειξη, με ημερομηνία, ώρα και ημερήσιο α/α έκδοσης στοιχείου.
1.4.4. Το λογισμικό υποστήριξης της ΕΑΦΔΣΣ που ευρίσκεται στον διασυνδεόμενο Η/Υ, λαμβάνει αυτή τη «μοναδική υπογραφή - κωδικό», και την εκτυπώνει μαζί με τα λοιπά δεδομένα του στοιχείου, ενώ συγχρόνως αποθηκεύει σε ιδιαίτερα ηλεκτρονικά αρχεία, τόσο το εκτυπωθέν στοιχείο, όσο και την «υπογραφή».
Η διαδικασία αυτή επαναλαμβάνεται για όλα τα στοιχεία του εκδότη.
1.4.5. Στο τέλος της ημέρας, ο ειδικός φορολογικός μηχανισμός σήμανσης, επεξεργάζεται το σύνολο των «κωδικών – υπογραφών» της μνήμης εργασίας, παράγει έναν γενικό ημερήσιο «κωδικό – υπογραφή» όλων των «κωδικών – υπογραφών» της ημέρας, εκδίδει δελτίο ημερήσιας αναφοράς «Ζ», στο οποίο αναγράφεται ο γενικός ημερήσιος «κωδικός – υπογραφή», αποθηκεύει τον «γενικό κωδικό - υπογραφή» σε ασφαλή φορολογική μνήμη που διαθέτει για το σκοπό αυτό, και τον αποστέλλει στον διασυνδεόμενο Η/Υ.
1.4.6. Το λογισμικό του Η/Υ, λαμβάνει αυτή τη «μοναδική γενική υπογραφή – κωδικό ημέρας», και την αποθηκεύει σε ιδιαίτερο ηλεκτρονικό αρχείο.

2. Επισημάνσεις

2.1. Το πρόβλημα της παράνομης αντιγραφής – αναπαραγωγής.

2.1.1. Το προτεινόμενο μέτρο δεν αποκλείει την παράνομη αναπαραγωγή εκδοθέντος δελτίου πχ μέσω φωτοτύπισης, αλλά είναι απολύτως βέβαιο, ότι στην περίπτωση ελέγχου και διαπίστωσης της ύπαρξης δύο ίδιων δελτίων, στα οποία αναγράφονται ακριβώς τα ίδια στοιχεία και φέρουν την ίδια σήμανση «υπογραφή - κωδικό», τότε το ένα από τα δύο είναι σίγουρα εικονικό – πλαστό και άρα παράνομο.
Η βεβαίωση της γνησιότητας (ή όχι) και της προέλευσης ενός εκδοθέντος δελτίου, γίνεται από τον έλεγχο των διαφυλασσομένων ηλεκτρονικών αρχείων του εκδότη καθώς και τον έλεγχο των αποθηκευμένων «υπογραφών» στον αντίστοιχο ειδικό φορολογικό μηχανισμό.

2.2. Η οδηγία 2001/115/ΕΚ της 20/12/2001 του Συμβουλίου της Ευρωπαϊκής Ένωσης για την τροποποίηση της οδηγίας 77/388/ΕΟΚ με στόχο την απλοποίηση, τον εκσυγχρονισμό και την εναρμόνιση των όρων που επιβάλλονται στην τιμολόγηση όσον αφορά το φόρο προστιθέμενης αξίας.

2.2.1. Η οδηγία αυτή, μεταξύ των άλλων, επιβάλλει την αναγραφή συγκεκριμένων μόνον ενδείξεων στα στοιχεία (τιμολόγια), και αρχικά ίσως προκύψει ερώτημα κατά πόσο το προτεινόμενο μέτρο της σήμανσης των στοιχείων είναι «συμβατό» με την οδηγία αυτή.
2.2.2. Η οδηγία αυτή επιβάλλει βέβαια την αναγραφή συγκεκριμένων μόνον στοιχείων στα τιμολόγια, αλλά όπως ρητά αναφέρεται «*...μόνον οι ακόλουθες ενδείξεις είναι υποχρεωτικές για τους σκοπούς του φόρου προστιθέμενης αξίας, όσον αφορά τα τιμολόγια που εκδίδονται...*» (σημ. η υπογράμμιση δική μας).
2.2.3. Το προτεινόμενο μέτρο, αφορά καθαρά την σήμανση για τον προσδιορισμό της γνησιότητας των στοιχείων και επομένως, εφόσον η χώρα μας αποδέχεται την αναγραφή των ενδείξεων της οδηγίας όσον αφορά τον ΦΠΑ, δεν φαίνεται να δημιουργείται κάποιο πρόβλημα σε σχέση με το σημείο αυτό.
2.2.4. Εξ άλλου μία από τις ενδείξεις που αναφέρονται στην οδηγία και θα πρέπει να αναγράφονται στα τιμολόγια είναι : « - *αλληλοδιάδοχος αριθμός, βασισμένος σε μια ή περισσότερες σειρές, ο οποίος χαρακτηρίζει το τιμολόγιο με μοναδικό τρόπο*» (σημ. η υπογράμμιση δική μας). Ο ειδικός ασφαλής αλγόριθμος που προτείνεται στο παρόν μέτρο, εξασφαλίζει απολύτως την απαίτηση αυτή της οδηγίας.
Τέλος η παρούσα πρόταση είναι απόλυτα συμβατή με τις αναφορές της οδηγίας για την διαφύλαξη των εκδοθέντων στοιχείων, μεταξύ των οποίων είναι και οι ακόλουθες *: « ...Η γνησιότητα της προέλευσης και η ακεραιότητα του περιεχομένου καθώς και το ευανάγνωστο αυτών των τιμολογίων πρέπει να εξασφαλίζονται για όλη της διάρκεια της αποθήκευσης. Όσον αφορά τα τιμολόγια που αναφέρονται στο στοιχείο γ) τρίτο εδάφιο, τα δεδομένα που περιέχουν δεν δύνανται να τροποποιηθούν, οφείλουν δε να παραμένουν ευανάγνωστα κατά τη διάρκεια της εν λόγω περιόδου. Τα κράτη μέλη καθορίζουν το χρονικό διάστημα κατά το οποίο οι υποκείμενοι στο φόρο οφείλουν να μεριμνούν για την αποθήκευση των τιμολογίων που αφορούν παραδόσεις αγαθών ή παροχές υπηρεσιών που πραγματοποιούνται στο έδαφός τους, καθώς και των τιμολογίων που λαμβάνονται από τους υποκείμενους στο φόρο που είναι εγκατεστημένοι στο έδαφός τους. Προκειμένου να εξασφαλίζεται η τήρηση των όρων που προβλέπονται στο τρίτο εδάφιο, τα κράτη μέλη που αναφέρονται στο τέταρτο εδάφιο δύνανται να επιβάλλουν την αποθήκευση των τιμολογίων με την αρχική τους μορφή με την οποία διαβιβάστηκαν, σε χαρτί ή με ηλεκτρονικά μέσα. Μπορούν επίσης να επιβάλλουν όπως, όταν τα τιμολόγια αποθηκεύονται με ηλεκτρονικά μέσα, τα δεδομένα που εξασφαλίζουν τη γνησιότητα της προέλευσης και την ακεραιότητα του περιεχομένου κάθε τιμολογίου να αποθηκεύονται και αυτά...».*
(σημ. η υπογράμμιση δική μας).

2.3. Ακεραιότητα και Κρυπτογράφηση δεδομένων.

Θα πρέπει εξ αρχής να γίνει κατανοητό ότι μάλλον δεν ενδιαφέρει τις φορολογικές αρχές αυτή καθεαυτή η Κρυπτογράφηση των δεδομένων. Το ενδιαφέρον των φορολογικών αρχών εστιάζεται μόνον στην ακεραιότητα των παραγόμενων δεδομένων - δελτίων και στην ευκολία δυνατότητας ελέγχου και επαλήθευσης, καθώς επίσης και της πιστοποίησης της αυθεντικότητας και της προέλευσης των δεδομένων αυτών.

- Πρόσβαση Δεδομένων :
  - ο Άμεση πρόσβαση στα στοιχεία
  - ο Γρήγορος εντοπισμός του σημείου ενδιαφέροντος
- Αυθεντικότητα Δεδομένων :
  - ο Άμεση δυνατότητα ελέγχου ακεραιότητας (μη αλλοίωσης).
  - ο Εύκολος προσδιορισμός της ταυτότητας και της προέλευσης.

Βέβαια θα πρέπει να σημειωθεί, ότι όλες αυτές οι παραπάνω απαιτήσεις θα μπορούσαν να υλοποιηθούν και μέσω της χρήσης αλγορίθμων και επιλογής κάποιων από τα διαθέσιμα standards κρυπτογράφησης. Όμως η κρυπτογράφηση παρουσιάζει ενδιαφέρον μόνον από την στιγμή που αποδειχθεί απαραίτητο εργαλείο για την επίτευξη των παραπάνω. Ιδιαίτερο πεδίο εφαρμογής της κρυπτογράφησης και της χρήσης «προηγμένης ηλεκτρονικής υπογραφής», θα μπορούσε πιθανόν να αποτελέσει η ηλεκτρονική μεταβίβαση -αποστολή και λήψη- των στοιχείων (ηλεκτρονικό εμπόριο), πράγμα που όμως μάλλον δεν μπορεί να εφαρμοστεί καθολικά και υποχρεωτικά στο άμεσο μέλλον.
Η περίπτωση όμως χρήσης της κρυπτογράφησης για τη σήμανση της πιστότητας των εκδιδόμενων στοιχείων και σε μια πιθανή προσέγγιση σε ασύμμετρους αλγόριθμους κρυπτογράφησης (με συνδυασμό ιδιωτικού-private και δημόσιου-public κλειδιού) , οι οποίοι γενικά θεωρούνται και οι ασφαλέστεροι, θα έθετε τις φορολογικές αρχές ενώπιον του προβλήματος μιας κεντρικής αποθήκευσης και διαχείρισης των δημόσιων κλειδιών και με ό,τι αυτό συνεπάγεται σε κόστος υλοποίησης και συντήρησης για το Δημόσιο. Επιπλέον δε, η υποχρεωτική απαίτηση για τη διασφάλιση του απόρρητου του ιδιωτικού κλειδιού, επαφίεται στις δυνατότητες και την καλή θέληση του κατόχου του.

2.4. Προσέγγιση απαιτούμενου χρόνου υλοποίησης – εφαρμογής του προτεινόμενου μέτρου.

2.4.1. Δεδομένου των απαιτούμενων τεχνολογικών καινοτομιών στην κατασκευή ειδικών ασφαλών φορολογικών διατάξεων/μηχανισμών σήμανσης στοιχείων (τόσο στο υλικό μέρος όσο και στο απαιτούμενο λογισμικό), της τήρησης των παραγωγικών διαδικασιών που εφαρμόζονται διεθνώς, απ' όλους σχεδόν τους κατασκευαστικούς οίκους, των διαδικασιών έγκρισης και χορήγησης αδειών καταλληλότητας και την κάλυψη των αναγκών της αγοράς που θα προκύψουν, ο προβλεπόμενος χρόνος έναρξης εφαρμογής του προτεινόμενου μέτρου, εκτιμάται κατά προσέγγιση από 6 έως 9 μήνες, από την δημοσίευση της σχετικής Υπουργικής απόφασης των Τεχνικών Προδιαγραφών που θα ισχύσουν με βάση το παρόν πόρισμα.

3. Ορισμοί – Βασικές Έννοιες

3.1. Ειδική Ασφαλής Φορολογική Διάταξη Σήμανσης Στοιχείων (ΕΑΦΔΣΣ).

3.1.1. Είναι αυτόνομη λειτουργικά και φυσικά συσκευή – φορολογικός μηχανισμός, ο οποίος περιλαμβάνει κατάλληλα ηλεκτρικά και ηλεκτρονικά κυκλώματα καθώς και το απαραίτητο λογισμικό, έχει τη δυνατότητα παραγωγής, καταγραφής σε εκτυπωτικό μηχανισμό και μόνιμης αποθήκευσης σε μνήμη ημιαγωγών μόνον αναγνώσεως (φορολογικής μνήμης), προηγμένης ασφαλούς ηλεκτρονικής ψηφιακής σύνοψης (ΠΑΗΨΣ) δεδομένων φορολογικών στοιχείων, και επικοινωνεί για τον σκοπό αυτό, διασυνδεόμενη μέσω κατάλληλης Ειδικής Θύρας Επικοινωνίας Δεδομένων (ΕΘΕΔ), με Ηλεκτρονικό Υπολογιστή.

3.2. Φορητή ΕΑΦΔΣΣ

3.2.1. Κάθε κατασκευαστής – εισαγωγέας ΕΑΦΔΣΣ, ο οποίος θέλει να λάβει άδεια καταλληλότητας συνδεόμενης ΕΑΦΔΣΣ με φορητό Η/Υ, σε περιβαλλοντικές συνθήκες λειτουργίας υπαίθρου, (απουσία δικτύου ηλεκτρικού ρεύματος, ειδικές συνθήκες υγρασίας και θερμοκρασίας) θα πρέπει να δηλώνει την πρόθεσή του αυτή ρητώς στην αίτηση – φάκελο αίτησης χορήγησης άδειας καταλληλότητας.

3.2.2. Η ΕΑΦΔΣΣ σ' αυτή την περίπτωση πληροί τις ειδικές απαιτήσεις περί φορητών Φορολογικών Ταμειακών Μηχανών (ΦΤΜ), όσον αφορά τις συνθήκες λειτουργίας περιβάλλοντος και ηλεκτρικής τροφοδοσίας, όπως περιγράφονται στις Τεχνικές Προδιαγραφές (ΑΥΟ 1144860/370/29.12.1998 – ΦΕΚ 1338/Β') και με βάση αυτές τις ειδικές απαιτήσεις, διενεργείται ο απαραίτητος έλεγχος στα εργαστήρια του ΕΜΠ. Στην περίπτωση αυτή η ΕΑΦΔΣΣ χαρακτηρίζεται ως «Φορητή ΕΑΦΔΣΣ».

3.3. Ειδική Θύρα Επικοινωνίας Δεδομένων - (ΕΘΕΔ)

3.3.1. Οι ΕΑΦΔΣΣ, διαθέτουν ολοκληρωμένη Ειδική Θύρα Επικοινωνίας Δεδομένων - (ΕΘΕΔ), για την επικοινωνία και μεταφορά δεδομένων από και προς το διασυνδεόμενο σύστημα Η/Υ. Η θύρα ΕΘΕΔ με την οποία συνδέεται η ΕΑΦΔΣΣ είναι συγκεκριμένη, και προσδιορίζεται ρητά από τον κατασκευαστή – εισαγωγέα της ΕΑΦΔΣΣ ως Ειδική Θύρα Επικοινωνίας Δεδομένων – ΕΘΕΔ με αντίστοιχη σήμανση επί ή πλησίον της θύρας αυτής.

3.4. Προηγμένη Ασφαλής Ηλεκτρονική Ψηφιακή Σύνοψη (ΠΑΗΨΣ).

3.4.1. Είναι μια αλληλουχία χαρακτήρων, η οποία δημιουργείται με την χρήση ειδικού ασφαλούς αλγόριθμου και η οποία προσδιορίζει μονοσήμαντα όλα τα δημοσιονομικά δεδομένα, κάθε εκδιδομένου στοιχείου, που επεξεργάζονται μέσω του αλγορίθμου αυτού.. Στην ουσία πρόκειται για ένα ηλεκτρονικό αποτύπωμα, που αποτελεί τη βάση ηλεκτρονικής υπογραφής – προηγμένης ηλεκτρονικής υπογραφής, όπως αυτή προσδιορίζεται στο άρθρο 2 της παραγράφου 2 του Π.Δ. 150/2001.

3.4.2. Για την δημιουργία της ΠΑΗΨΣ, γίνεται χρήση του ειδικού ασφαλούς αλγορίθμου SHA-1. Με τον αλγόριθμο SHA-1, η παραγόμενη ΠΑΗΨΣ, σχηματίζεται από 40 σύμβολα – χαρακτήρες του δεκαεξαδικού αριθμητικού συστήματος (20 Bytes).

Σημ.

Η υλοποίηση της ΠΑΗΨΣ είναι δυνατό να γίνει με χρήση διαφόρων αλγορίθμων, αλλά για λόγους διευκόλυνσης και κοινού τρόπου ελέγχου της γνησιότητας των υπογεγραμμένων δεδομένων, επιβάλλεται η υιοθέτηση ενός κοινά αποδεκτού αλγορίθμου.
Ο αλγόριθμος αυτός είναι ο SHA-1 (Secure Hash Algorithm - 1), ο οποίος αποτελεί ένα από τα πλέον ασφαλή διεθνή πρότυπα, έχει αναπτυχθεί από το Αμερικανικό Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας - NIST (National Institute of Standards and Technology), και έχει υιοθετηθεί από τον Διεθνή Οργανισμό Προτύπων - ISO (International Organization for Standardization) και την Διεθνή Ηλεκτροτεχνική Επιτροπή - IEC (International Electrotechnical Commission), ως πρότυπο ISO/IEC 10118 – 3, Dedicated Hash-Function 3.
Σχετικά στοιχεία για τον αλγόριθμο SHA-1, παρατίθεται στο Παράρτημα Π1,σε κείμενο στην ελληνική γλώσσα, το οποίο βασίζεται στο έγγραφο – πρότυπο FIPS-180-2 (Federal Information Processing Standards) που εκδόθηκε από το National Institute of Standards and Technology (NIST) μετά την υιοθέτησή του από το Υπουργείο των ΗΠΑ (Secretary of Commerce) σύμφωνα με την παράγραφο 5131 του Information Technology Management Reform Act of 1996 (Public Law 104-106), και του Computer Security Act of 1987 (Public Law 100-235) των Ηνωμένων Πολιτειών Αμερικής.

3.5. Δελτίο Φορολογικής Σήμανσης Στοιχείου (ΔΦΣΣ).

3.5.1. Η ΕΑΦΔΣΣ μετά από κάθε λήψη φορολογικών δεδομένων για την έκδοση στοιχείου από τον διασυνδεόμενο Η/Υ και την επεξεργασία αυτών μέσω του ειδικού ασφαλούς αλγορίθμου SHA-1 δημιουργίας σύνοψης – υπογραφής, εκδίδει σχετικό δελτίο – απόδειξη, το οποίο ονομάζεται Δελτίο Φορολογικής Σήμανσης Στοιχείου (ΔΦΣΣ), και στο οποίο αναγράφονται :

- ημερομηνία και ώρα έκδοσης του δελτίου
- ο ημερήσιος α/α του εκδιδόμενου Δελτίου Φορολογικής Σήμανσης Στοιχείου.
- ο γενικός α/α (από αρχής λειτουργίας της ΕΑΦΔΣΣ) του εκδιδόμενου Δελτίου Φορολογικής Σήμανσης Στοιχείου
- Η ΠΑΗΨΣ του συγκεκριμένου στοιχείο

3.5.2. Τα δελτία αυτά φυλάσσονται με ευθύνη του κατόχου της ΕΑΦΔΣΣ μέχρι της εκδόσεως του **Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων - «Z»** που αφορά την αντίστοιχη ημέρα εκδόσεώς τους.

3.5.3. Στην ακραία περίπτωση εμφάνισης βλάβης της μνήμης εργασίας (CMOS Error) της ΕΑΦΔΣΣ, τα δελτία αυτά φυλάσσονται μέχρι αποκαταστάσεως της βλάβης, επανατροφοδοτήσεως τους στην ΕΑΦΔΣΣ και τελικής εκδόσεως του σχετικού **Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων - «Z»**, επιδεικνύονται δε σε κάθε περίπτωση ελέγχου των φορολογικών αρχών, ως αποδεικτικά εκδόσεως των αντίστοιχων στοιχείων.

3.6. Δελτίο Συνόψεων - Υπογραφών Ημέρας (ΔΣΥΜ)

3.6.1. Η ΕΑΦΔΣΣ έχει δυνατότητα μέσω κατάλληλων χειρισμών, έκδοσης ενός δελτίου αναφοράς όλων των, μέχρι τη στιγμή της έκδοσης του δελτίου αυτού, συνόψεων – υπογραφών ημέρας.

3.6.2. Το δελτίο αυτό ονομάζεται Δελτίο Συνόψεων - Υπογραφών Ημέρας - (ΔΣΥΜ) και σ' αυτό αναγράφονται όλες οι ΠΑΗΨΣ για κάθε εκδοθέν στοιχείο, που έχουν γίνει εντός της ημέρας (από την έκδοση του προηγούμενου **Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων - «Z»),** ως εξής:

- ημερομηνία και ώρα έκδοσης του δελτίου
- ο ημερήσιος α/α του εκδιδόμενου Δελτίου Φορολογικής Σήμανσης Στοιχείου.
- ο γενικός α/α (από αρχής λειτουργίας της ΕΑΦΔΣΣ) του εκδιδόμενου Δελτίου Φορολογικής Σήμανσης Στοιχείου
- Η ΠΑΗΨΣ του συγκεκριμένου στοιχείου

3.7. Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων (ΔΗΦΑΣΣ) – «Z».

3.7.1. Η ΕΑΦΔΣΣ στο τέλος της ημέρας, επεξεργάζεται το σύνολο των «συνόψεων – υπογραφών» της μνήμης εργασίας μέσω του ειδικού ασφαλούς αλγορίθμου SHA-1, παράγει μια γενική ημερήσια «σύνοψη – υπογραφή» και εκδίδει σχετικό δελτίο «Z» το οποίο ονομάζεται Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ).

3.7.2. Με το πέρας της εκδόσεως του δελτίου αυτού, μηδενίζονται τα δεδομένα της μνήμης εργασίας. Στο Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) αναγράφονται :

- ημερομηνία και ώρα έκδοσης του δελτίου
- ο γενικός α/α (από αρχής λειτουργίας της ΕΑΦΔΣΣ) του εκδιδόμενου Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων - «Z»
- όλες οι ΠΑΗΨΣ για κάθε εκδοθέν στοιχείο, που έχουν γίνει εντός της ημέρας (από την έκδοση του προηγούμενου Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων - «Z»), ως εξής:
  - ο ημερήσιος α/α του εκδιδόμενου Δελτίου Φορολογικής Σήμανσης Στοιχείου.
  - ο γενικός α/α (από αρχής λειτουργίας της ΕΑΦΔΣΣ) του εκδιδόμενου Δελτίου Φορολογικής Σήμανσης Στοιχείου
  - Η ΠΑΗΨΣ του συγκεκριμένου στοιχείου
- Η Γενική Ημερήσια «σύνοψη – υπογραφή» των ΠΑΗΨΣ της ημέρας.
- Ο Ημερήσιος και ο Γενικός (από αρχής λειτουργίας της ΕΑΦΔΣΣ) α/α αριθμός Αποσυνδέσεων της ΕΑΦΔΣΣ.
- Ο Ημερήσιος και ο Γενικός (από αρχής λειτουργίας της ΕΑΦΔΣΣ) α/α αριθμός Βλαβών Μνήμης Εργασίας (CMOS-Error).
- Ο Ημερήσιος και ο Γενικός (από αρχής λειτουργίας της ΕΑΦΔΣΣ) α/α αριθμός Αλλαγών Λεκτικών Επωνυμίας Κατόχου.
- Ο Ημερήσιος και ο Γενικός (από αρχής λειτουργίας της ΕΑΦΔΣΣ) α/α αριθμός προσβάσεων – επεμβάσεων εξουσιοδοτημένου Τεχνικού .

3.7.3. Δεν επιτρέπεται η χρήση του διακριτικού γράμματος «Z», εμφανώς σε τίτλο ή επικεφαλίδα κανενός άλλου εκδιδόμενο δελτίο πλην του Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου (ΔΗΦΑΣΣ) - «Z», με το οποίο γίνεται η εγγραφή της γενικής σύνοψης των ΠΑΗΨΣ της ημέρας και λοιπών ημερήσιων αθροιστών προοδευτικά και σωρευτικά στη φορολογική μνήμη.

3.8. Δελτίο Ανάγνωσης Περιόδου Φορολογικής Μνήμης Ημερήσιων Συνόψεων– (ΔΑΠΦΜΗΣ)

3.8.1. Η ΕΑΦΔΣΣ έχει δυνατότητα μέσω κατάλληλων χειρισμών, έκδοσης δελτίου αναφοράς όλων των Δελτίων Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου «Z» – (ΔΗΦΑΣΣ), το οποίο ονομάζεται Δελτίο Ανάγνωσης Περιόδου Φορολογικής Μνήμης Ημερήσιων Συνόψεων – (ΔΑΠΦΜΗΣ).
3.8.2. Η έκδοση του δελτίου αυτού γίνεται ημερολογιακά από ημερομηνία έως ημερομηνία ή εναλλακτικά από α/α δελτίου ΔΗΦΑΣΣ - «Z» έως α/α δελτίου ΔΗΦΑΣΣ - «Z».
3.8.3. Στο δελτίο αυτό αναγράφονται :

- ημερομηνία και ώρα έκδοσης του δελτίου
- όλες οι Γενικές Ημερήσιες ΠΑΗΨΣ για κάθε εκδοθέν Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων - «Z»), της συγκεκριμένης περιόδου, ως εξής:
  - ο α/α του Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων - «Z».
  - ο συνολικός αριθμός των εκδοθέντων και «υπογραφέντων» στοιχείων της ημέρας.
  - η Γενική Ημερήσια «σύνοψη – υπογραφή» του αντίστοιχου ΔΗΦΑΣΣ-«Z».
- ο α/α αριθμός Αποσυνδέσεων της ΕΑΦΔΣΣ της συγκεκριμένης περιόδου.
- ο α/α αριθμός Βλαβών Μνήμης Εργασίας (CMOS-Error) της συγκεκριμένης περιόδου.
- ο α/α αριθμός Αλλαγών Λεκτικών Επωνυμίας Κατόχου της συγκεκριμένης περιόδου.
- ο α/α αριθμός προσβάσεων – επεμβάσεων εξουσιοδοτημένου Τεχνικού της συγκεκριμένης περιόδου.

3.9. Ειδικά Φορολογικά Δελτία

3.9.1 Τα δελτία : 1. Δελτίο Φορολογικής Σήμανσης Στοιχείου (ΔΦΣΣ), 2. Δελτίο Συνόψεων - Υπογραφών Ημέρας (ΔΣΥΜ), 3. Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων (ΔΗΦΑΣΣ) – «Z» και 4. Δελτίο Ανάγνωσης Περιόδου Φορολογικής Μνήμης Ημερήσιων Συνόψεων – (ΔΑΠΦΜΗΣ), ονομάζονται «Ειδικά Φορολογικά Δελτία» (ΕΦΔ) και η έκδοσή τους υποχρεωτικά περιλαμβάνει στην αρχή και στο τέλος της εκτύπωσης κάθε τέτοιου δελτίου, τις χαρακτηριστικές ενδείξεις «Ειδικό Φορολογικό Δελτίο - Έναρξη» και «Ειδικό Φορολογικό Δελτίο - Λήξη», αντίστοιχα.

3.9.2. Μετά την χαρακτηριστική ένδειξη «Ειδικό Φορολογικό Δελτίο - Έναρξη» αναγράφονται υποχρεωτικά τα στοιχεία του κατόχου – ιδιοκτήτη της ΕΑΦΔΣΣ, ως εξής :

- Ονοματεπώνυμο, πατρώνυμο ή επωνυμία
- Διεύθυνση εγκατάστασης στην οποία λειτουργεί η ΕΑΦΔΣΣ
- Επάγγελμα – Δραστηριότητα
- ΑΦΜ και αρμόδια ΔΟΥ

3.9.3. Πριν ακριβώς από την χαρακτηριστική ένδειξη «Ειδικό Φορολογικό Δελτίο - Λήξη» αναγράφεται υποχρεωτικά ο αριθμός Μητρώου της ΕΑΦΔΣΣ.

4. Λογισμικό Η/Υ.

4.1. Λογισμικό εκδότη στοιχείων - Γενικά

Το λογισμικό του διασυνδεόμενου Η/Υ, του εκδότη φορολογικών στοιχείων, εκτός της διαχείρισης και επεξεργασίας των δημοσιονομικών δεδομένων και εκτύπωσης των φορολογικών στοιχείων, έχει επιπλέον δυνατότητες υποστήριξης και συνεργασίας με την διασυνδεόμενη ΕΑΦΔΣΣ :

- αποθήκευσης των εκδοθέντων φορολογικών στοιχείων και των αντίστοιχων ΠΑΗΨΣ σε αρχεία ηλεκτρονικής μορφής.
- αποστολής των προς εκτύπωση φορολογικών στοιχείων για υπογραφή προς την ΕΑΦΔΣΣ
- λήψης από την ΕΑΦΔΣΣ του Αρ. μητρώου της καθώς και του γενικού και ημερήσιου α/α έκδοσης στοιχείου.
- λήψης της παραχθείσας ΠΑΗΨΣ από την ΕΑΦΔΣΣ
- σήμανσης των εκτυπούμενων δελτίων των στοιχείων αυτών, με την αναγραφή - αποτύπωση της ΠΑΗΨΣ στα δελτία αυτά και την τελική εκτύπωση – έκδοσή τους.
- επανατροφοδοτήσεως της ΕΑΦΔΣΣ με τα δεδομένα δημιουργίας ΠΑΗΨΣ, μετά από ακραία περίπτωση εμφάνισης βλάβης της μνήμης εργασίας (CMOS Error) της ΕΑΦΔΣΣ.
- ανιχνεύσεως κάθε περίπτωση αποσύνδεσης της ΕΑΦΔΣΣ, στις περιπτώσεις αποστολής ή λήψης δεδομένων προς και από αυτήν.

Σημ.
Σε αρχική προσέγγιση της πρότασης εφαρμογής του μέτρου, υπήρχε και σχετική παράγραφος για επιπλέον Αποτύπωση της ΠΑΗΨΣ και με Γραμμωτό Κώδικα (Bar Code), ώστε να διευκολύνεται για την μηχανογραφική εισαγωγή – καταχώρησή της, ο αποδέκτης των στοιχείων.
Επίσης στην προσέγγιση της πρότασης εφαρμογής του μέτρου, υπήρχε και η αντίστοιχη σχετική παράγραφος για το Λογισμικό αποδέκτη στοιχείων, το οποίο θα έπρεπε να έχει δυνατότητα καταχώρησης των λαμβανομένων ΠΑΗΨΣ των στοιχείων.
Και οι δύο παράγραφοι αποσκοπούσαν στη διευκόλυνση μια πιθανής μελλοντικής ασφαλούς διασταύρωσης στοιχείων.
Οι παράγραφοι αυτοί θεωρήθηκε ότι θα πρέπει να αποσυρθούν από την αρχική πρόταση εφαρμογής του μέτρου, λόγω του χρόνου – κόστους καταχώρησης, καθώς και επειδή η εφαρμογή τους, περιορίζεται μόνον από όσους αποδέκτες στοιχείων κάνουν χρήση Η/Υ για την καταχώρησή τους.

4.2. Περιπτώσεις Λογισμικού Υποστήριξης

Για την λειτουργία – συνεργασία της ΕΑΦΔΣΣ με ήδη εγκατεστημένο λογισμικό εφαρμογών έκδοσης στοιχείων Η/Υ διακρίνονται δύο περιπτώσεις :

Α.
4.2.1. Ειδικό Λογισμικό Υποστήριξης

4.2.1.1. Ο κάτοχος άδειας καταλληλότητας ΕΑΦΔΣΣ διαθέτει δικό του ειδικό λογισμικό υποστήριξης και συνεργασίας (driver), το οποίο λειτουργεί σε επίπεδο λειτουργικού συστήματος Η/Υ και αναλαμβάνει όλη την διαχείριση και συνεργασία μεταξύ του λογισμικού εφαρμογών έκδοσης – εκτύπωσης στοιχείων και της ΕΑΦΔΣΣ.

4.2.1.2. Το ειδικό αυτό λογισμικό, επιτελεί τις εξής λειτουργίες και έχει τις εξής δυνατότητες:
1. Έχει δυνατότητα ενεργοποίησης και απενεργοποίησης της λειτουργίας του, από χειριστή.
2. Έχει δυνατότητα επιλογής – καθορισμού από τον χειριστή, ήδη εγκατεστημένης - σε επίπεδο λειτουργικού συστήματος- εκτυπωτικής συσκευής με την οποία μπορεί να συνεργάζεται.
3. Ανιχνεύει τις αιτήσεις εκτύπωσης εφαρμογών του λειτουργικού συστήματος, οι οποίες απευθύνονται προς την επιλεγμένη εκτυπωτική συσκευή με την οποία συνεργάζεται.
4.Δέχεται το σύνολο των προς εκτύπωση δεδομένων προς την επιλεγμένη εκτυπωτική συσκευή, τα επεξεργάζεται και αποστέλλει το σύνολο των δεδομένων που απαιτούνται για την δημιουργία της ΠΑΗΨΣ κάθε στοιχείου, προς την διασυνδεόμενη ΕΑΦΔΣΣ.
5. Αποθηκεύει τα δεδομένα αυτά σε ηλεκτρονικό αρχείο κειμένου, του οποίου ο τρόπος ονοματοδοσίας καθώς και το μέσο αποθήκευσης μπορούν να προκαθορίζονται από τον χειριστή.
6. Δέχεται από την ΕΑΦΔΣΣ :
- την ΠΑΗΨΣ
- τον γενικό και ημερήσιο α/α σήμανσης – έκδοσης στοιχείου
- τον Αρ. Μητρώου της ΕΑΦΔΣΣ

7. Αποθηκεύει τα δεδομένα που έχει δεχθεί από την ΕΑΦΔΣΣ σε ηλεκτρονικό αρχείο μιας συμβολοσειράς κειμένου σταθερού μήκους (η οποία περιλαμβάνει τα στοιχεία του προηγούμενου σημείου 6), του οποίου ο τρόπος ονοματοδοσίας καθώς και το μέσο αποθήκευσης μπορούν να προκαθορίζονται από τον χειριστή.
8. Στο σύνολο των προς εκτύπωση δεδομένων, προσθέτει μια επιπλέον γραμμή, η οποία αποτελείται από μια συμβολοσειρά σταθερού μήκους η οποία περιλαμβάνει τα στοιχεία του προηγούμενου σημείου 6, και τα εκτυπώνει στην επιλεγμένη συσκευή εκτύπωσης.

4.2.1.3. Επιπλέον το ειδικό αυτό λογισμικό έχει δυνατότητα επανατροφοδοτήσεως της ΕΑΦΔΣΣ με τα δεδομένα δημιουργίας ΠΑΗΨΣ, μετά από ακραία περίπτωση εμφάνισης βλάβης της μνήμης εργασίας (CMOS Error) της ΕΑΦΔΣΣ, καθώς και ανίχνευσης κάθε περίπτωσης αποσύνδεσης ή μή δυνατότητας επικοινωνίας σε κατάσταση αποστολής ή λήψης δεδομένων προς ή από την διασυνδεόμενη ΕΑΦΔΣ .

4.2.1.4. Στην περίπτωση αυτή, το ειδικό αυτό λογισμικό αποτελεί αναπόσπαστο τμήμα της ΕΑΦΔΣΣ και της έγκρισής της.

Β.

4.2.2. Ήδη εγκατεστημένο λογισμικό εφαρμογών έκδοσης στοιχείων με κατάλληλη τροποποίηση.

4.2.2.1. Το ήδη εγκατεστημένο λογισμικό εφαρμογών έκδοσης στοιχείων Η/Υ, με κατάλληλη τροποποίηση, αναλαμβάνει όλη την διαχείριση και συνεργασία μεταξύ αυτού και της ΕΑΦΔΣΣ.

4.2.2.1.1. Στην περίπτωση αυτή το λογισμικό εφαρμογών επιτελεί τις λειτουργίες και έχει τις εξής δυνατότητες :

1. Αποθηκεύει τα προς εκτύπωση στοιχεία σε ηλεκτρονικά αρχεία κειμένου, των οποίων ο τρόπος ονοματοδοσίας καθώς και το μέσο αποθήκευσης μπορούν να προκαθορίζονται από τον χειριστή.
2. Επεξεργάζεται και αποστέλλει το σύνολο των δεδομένων που απαιτούνται για την δημιουργία της ΠΑΗΨΣ κάθε στοιχείου, προς την διασυνδεόμενη ΕΑΦΔΣΣ.
3. Δέχεται από την ΕΑΦΔΣΣ :

- την ΠΑΗΨΣ για κάθε συγκεκριμένο στοιχείο
- τον γενικό και ημερήσιο α/α σήμανσης – έκδοσης στοιχείου
- τον Αρ. Μητρώου της ΕΑΦΔΣΣ

4. Αποθηκεύει τα δεδομένα που έχει δεχθεί από την ΕΑΦΔΣΣ σε ηλεκτρονικό αρχείο μιας συμβολοσειράς κειμένου σταθερού μήκους (η οποία περιλαμβάνει τα στοιχεία του προηγούμενου σημείου 3), του οποίου ο τρόπος ονοματοδοσίας καθώς και το μέσο αποθήκευσης μπορούν να προκαθορίζονται από τον χειριστή.
5. Στο σύνολο των προς εκτύπωση δεδομένων, προσθέτει μια επιπλέον γραμμή, η οποία αποτελείται από μια συμβολοσειρά σταθερού μήκους η οποία περιλαμβάνει τα στοιχεία του προηγούμενου σημείου 3, και τα εκτυπώνει στην επιλεγμένη συσκευή εκτύπωσης.

4.2.2.1.2. Επιπλέον το λογισμικό αυτό έχει δυνατότητα επανατροφοδοτήσεως της ΕΑΦΔΣΣ με τα δεδομένα δημιουργίας ΠΑΗΨΣ, μετά από ακραία περίπτωση εμφάνισης βλάβης της μνήμης εργασίας (CMOS Error) της ΕΑΦΔΣΣ, καθώς και ανίχνευσης κάθε περίπτωσης αποσύνδεσης ή μη δυνατότητας επικοινωνίας σε κατάσταση αποστολής ή λήψης δεδομένων προς ή από την διασυνδεόμενη ΕΑΦΔΣ .

4.2.2.1.3. Σ’ αυτή την περίπτωση (**Β.**), ο κάτοχος της άδειας καταλληλότητας ΕΑΦΔΣΣ, υποχρεούται στην έγγραφη δεσμευτική διαβεβαίωση του, προς την Επιτροπή, περί του ελέγχου και της πιστοποίησης της ορθής λειτουργίας του χρησιμοποιούμενου (συνεργαζόμενου) λογισμικού εφαρμογών έκδοσης στοιχείων του διασυνδεομένου Η/Υ, ότι αυτό εκδίδει τα στοιχεία απολύτως σύμφωνα με τις ισχύουσες σχετικές διατάξεις του Κ.Β.Σ. και των αρμοδίων υπηρεσιών του Υπουργείου Οικονομίας και Οικονομικών και δεν παρακάμπτει με κανένα τρόπο το σύστημα ασφάλειας των δημοσιονομικών δεδομένων του συγκεκριμένου ΕΑΦΔΣΣ.
Στην δεσμευτική διαβεβαίωση – πιστοποίηση του λογισμικού εφαρμογών έκδοσης στοιχείων, αναφέρονται υποχρεωτικά :

- Τα πλήρη στοιχεία του κατασκευαστή του λογισμικού εφαρμογών.
- Η ακριβής ονομασία διάθεσης και ο τρέχων αριθμός έκδοσης (version) του λογισμικού αυτού.

Η δεσμευτική διαβεβαίωση – πιστοποίηση προς την Επιτροπή, γίνεται για κάθε διαφορετικό λογισμικό που πρόκειται να χρησιμοποιείται και συνοδεύεται από ένα αντίγραφο έκδοσης επίδειξης του λογισμικού αυτού, αποθηκευμένο σε κατάλληλο μαγνητικό ή οπτικό μέσο, καθώς και πλήρη στοιχεία για τις απαιτήσεις και συνθήκες λειτουργίας του, σε Ηλεκτρονικό Υπολογιστή.

4.2.2.1.4. Τα στοιχεία αυτά συμπληρώνονται σε ειδικό τμήμα σελίδων, που υπάρχει για τον σκοπό αυτό στο συνοδευτικό του ΕΑΦΔΣΣ, Βιβλιάριο Συντήρησης και Επισκευών.

4.2.2.1.5. Ο κάτοχος της άδειας καταλληλότητας ΕΑΦΔΣΣ και το δίκτυο των εξουσιοδοτημένων αντιπροσώπων του, σε οποιαδήποτε περίπτωση διαπίστωσης

παράβασης των ανωτέρω, είναι υποχρεωμένοι στην άμεση γνωστοποίηση του γεγονότος αυτού στην αρμόδια ΔΟΥ του κατόχου του ΕΑΦΔΣΣ και στην Επιτροπή.

4.3. Δημιουργία, αποθήκευση και διαφύλαξη Ηλεκτρονικών Αρχείων (Κειμένου δελτίου Στοιχείου και αντίστοιχης ΠΑΗΨΣ)

4.3.1. Δημιουργούμενα αρχεία σε Ηλεκτρονικό Υπολογιστή

4.3.1.1. Μετά την ολοκλήρωση της επικοινωνίας μεταξύ της ΕΑΦΔΣΣ και του διασυνδεόμενου Η/Υ, για την σήμανση κάθε στοιχείου, δημιουργούνται από το λογισμικό υποστήριξης της ΕΑΦΔΣΣ, και αποθηκεύονται στον Η/Υ σε κατάλληλο μαγνητικό ή οπτικό αποθηκευτικό μέσο, 2 ηλεκτρονικά αρχεία, σε μορφή απλού αναγνώσιμου κειμένου ΕΛΟΤ-928.

4.3.1.2. Το πρώτο εξ αυτών αποτελεί το ηλεκτρονικό αρχείο των δεδομένων του συγκεκριμένου εκδοθέντος στοιχείου. Το περιεχόμενο του αρχείου αυτού αποτελείται μόνον από τους χαρακτήρες – σύμβολα που έχουν αποκλειστικά συμμετάσχει στο σχηματισμό της ΠΑΗΨΣ του στοιχείου. Στον σχηματισμό της ονομασίας αυτού του αρχείου συμμετέχουν :
α) ο 11-ψήφιος (τα 3 γράμματα έγκρισης + τα 8 ψηφία του αριθμού παραγωγής χωρίς ενδιάμεσα κενά) αριθμός μητρώου της ΕΑΦΔΣΣ από την οποία έχει προέλθει,
β) τα 6 ψηφία της ημερομηνίας δημιουργίας του (εγγραφής του) ως εξής : YYMMDD, όπου YY είναι το έτος, ο μήνας MM και DD η ημερομηνία,
γ) ο ημερήσιος αύξων αριθμός σήμανσης – έκδοσης στοιχείου σε μορφή μετρητή σταθερού μήκους 4 ψηφίων. Ο α/α αναγράφεται στο δεξιότερο μέρος και οι τυχόν υπόλοιπες θέσεις (μέχρι τον αριθμό 4) των ψηφίων συμπληρώνονται με 0. Δεν παρεμβάλλεται κανένα σύμβολο διαχωρισμού τριάδων (εκατοντάδων, χιλιάδων κλπ).,
δ) το σύμβολο της κάτω παύλας (“_” underscore) ακολουθούμενο από το ενδεικτικό λατινικό γράμμα “a”, καθώς και
ε) το προέκταμα «.txt» που υποδηλώνει το είδος του (απλό αναγνώσιμο ΕΛΟΤ-928).

4.3.1.3. Το δεύτερο εξ αυτών αποτελεί το ηλεκτρονικό αρχείο της ΠΑΗΨΣ του συγκεκριμένου στοιχείου. Στον σχηματισμό της ονομασίας αυτού του αρχείου αυτού συμμετέχουν :
α) ο 11-ψήφιος (τα 3 γράμματα έγκρισης + τα 8 ψηφία του αριθμού παραγωγής χωρίς ενδιάμεσα κενά) αριθμός μητρώου της ΕΑΦΔΣΣ από την οποία έχει προέλθει,
β) τα 6 ψηφία της ημερομηνίας δημιουργίας του (εγγραφής του) ως εξής : YYMMDD, όπου YY είναι το έτος, ο μήνας MM και DD η ημερομηνία,
γ) ο ημερήσιος αύξων αριθμός σήμανσης – έκδοσης στοιχείου σε μορφή μετρητή σταθερού μήκους 4 ψηφίων. Ο α/α αναγράφεται στο δεξιότερο μέρος και οι τυχόν υπόλοιπες θέσεις (μέχρι τον αριθμό 4) των ψηφίων συμπληρώνονται με 0. Δεν παρεμβάλλεται κανένα σύμβολο διαχωρισμού τριάδων (εκατοντάδων, χιλιάδων κλπ).,
δ) το σύμβολο της κάτω παύλας (“_” underscore) ακολουθούμενο από το ενδεικτικό λατινικό γράμμα “b”, καθώς και
ε) το προέκταμα «.txt» που υποδηλώνει το είδος του (απλό αναγνώσιμο ΕΛΟΤ-928).

4.3.1.4. Στο δεύτερο αυτό αρχείο, το οποίο έχει πάντα σταθερό μέγεθος 67 χαρακτήρων, περιέχονται μόνον :

- η αλληλουχία των 40 δεκαεξαδικών ΕΛΟΤ-928 χαρακτήρων της αντίστοιχης ΠΑΗΨΣ του στοιχείου (γίνεται χρήση μόνον αριθμών και κεφαλαίων λατινικών χαρακτήρων A…F).
- ένας κενός χαρακτήρας (διάστημα - space)
- ο ημερήσιος αύξων αριθμός σήμανσης – έκδοσης στοιχείου σε μορφή μετρητή σταθερού μήκους 4 ψηφίων. Ο α/α αναγράφεται στο δεξιότερο μέρος και οι τυχόν υπόλοιπες θέσεις (μέχρι τον αριθμό 4) των ψηφίων συμπληρώνονται με 0. Δεν παρεμβάλλεται κανένα σύμβολο διαχωρισμού τριάδων (εκατοντάδων, χιλιάδων κλπ).
- ένας κενός χαρακτήρας (διάστημα - space)
- ο γενικός α/α σήμανσης – έκδοσης στοιχείου σε μορφή μετρητή σταθερού μήκους 8 ψηφίων. Ο α/α αναγράφεται στο δεξιότερο μέρος και οι τυχόν υπόλοιπες θέσεις (μέχρι τον αριθμό 8) των ψηφίων συμπληρώνονται με 0. Δεν παρεμβάλλεται κανένα σύμβολο διαχωρισμού τριάδων (εκατοντάδων, χιλιάδων κλπ).
- ένας κενός χαρακτήρας (διάστημα - space)
- ο Αρ. Μητρώου της ΕΑΦΔΣΣ (3 χαρακτήρες – γράμματα του αριθμού έγκρισης, ένας κενός χαρακτήρας (διάστημα - space), και ο α/α εργοστασιακός σειριακός αριθμός παραγωγής ο οποίος επίσης είναι σταθερού μεγέθους και σχηματίζεται από 8 ψηφία).

4.3.2. **Για την υποχρέωση και το σκοπό διαφύλαξης των αποθηκευμένων Ηλεκτρονικών Αρχείων.**

4.3.2.1. Τα εν λόγω δημιουργούμενα αρχεία, (του κειμένου του δελτίου του εκδιδομένου στοιχείου και της ΠΑΗΨΣ που αντιστοιχεί σ' αυτό), με αποκλειστική ευθύνη του κατόχου της ΕΑΦΔΣΣ και υπόχρεου στη φύλαξη στοιχείων, φυλάσσονται για όσο χρονικό διάστημα ορίζουν οι φορολογικές διατάξεις του άρθρου 21 του Κ.Β.Σ. (6 χρόνια), παραμένουν δε, άμεσα προσπελάσιμα και αναγνώσιμα σε οποιαδήποτε απαίτηση των φορολογικών αρχών και παρέχεται κάθε διευκόλυνση και εφόδιο (μέσα, αναγκαίος εξοπλισμός κλπ), για την μεταφορά τους σε άλλο προσωπικό ηλεκτρονικό υπολογιστή και την διενέργεια σχετικών εκτυπώσεων και ελέγχων επαλήθευσης.

4.3.2.2. Οποιαδήποτε απώλεια η αλλοίωση του αρχείου αυτού, επισύρει τις προβλεπόμενες από τις σχετικές διατάξεις κυρώσεις (άρθρο 30 Κ.Β.Σ. και άρθρο 5 του ν. 2523/1997).

4.3.2.3. Η γνησιότητα της προέλευσης και η διατήρηση της ακεραιότητας του περιεχομένου καθώς και η αναγνωσιμότητα των στοιχείων των αρχείων αυτών πρέπει να εξασφαλίζονται για όλη της διάρκεια της αποθήκευσής τους.

5. Δεδομένα Δημιουργίας ΠΑΗΨΣ

5.1. Χρήση συγκεκριμένης κωδικοποίησης – κωδικοσελίδας.

5.1.1. Για τον σχηματισμό της ΠΑΗΨΣ κάθε εκδιδομένου στοιχείου, αλλά και της γενικής ημερήσιας ΠΑΗΨΣ, ακολουθείται το πρότυπο της θέσης / σειράς των χαρακτήρων – συμβόλων, ΕΛΟΤ-928, ανεξάρτητα από την εσωτερική παράσταση εντός της ΕΑΦΔΣΣ, των εκτυπούμενων συμβόλων και χαρακτήρων.

5.2. Ειδικοί χαρακτήρες – χαρακτήρες ελέγχου μορφοποίησης

5.2.1. Στην περίπτωση που η εκτύπωση των δελτίων των εκδιδομένων στοιχείων περιλαμβάνει και άλλους ειδικούς χαρακτήρες μορφοποίησης κειμένου (πχ έντονης γραφής, διπλού ύψους, πλάτους, κλίσης συμβόλων, χρώματος, οριζοντίων ή καθέτων γραμμών κλπ), τότε αυτοί δεν αποστέλλονται στην ΕΑΦΔΣΣ και δεν συμμετέχουν στον σχηματισμό της ΠΑΗΨΣ του στοιχείου.

5.2.2. Δεν απαιτείται η εμφάνιση και η μορφοποίηση (έντονη γραφή, διπλό ύψος, κλίση γραμμάτων, εικόνες, γραφικά κλπ) στο κειμένου που περιέχεται (και μπορεί να εκτυπώνεται), από το μόνιμα αποθηκευμένο στον Η/Υ αρχείο του συγκεκριμένου στοιχείου, να ταυτίζεται απόλυτα στην μορφή με το εκδοθέν.

5.3. Χρήση Γραφικών - Εικόνων.

5.3.1. Στην περίπτωση που στην εκτύπωση των δελτίων των εκδιδομένων στοιχείων γίνεται χρήση διαφημιστικών σε μορφή γραφικών ή εικόνας, τότε για τον σχηματισμό της ΠΑΗΨΣ, τα δεδομένα που αφορούν την εικόνα ή το γραφικό, αντικαθίστανται από την ενδεικτική λέξη «[Εικόνα]», μέσα σε όρθιες αγκύλες.

5.3.2. Εάν γίνεται χρήση εικόνων ή γραφικών, τότε αυτά δεν επιτρέπεται να έχουν αναφορές σε ποσά ή να παραπλανούν ή να παραπέμπουν σε οποιεσδήποτε παρανοήσεις των δεδομένων του εκδιδομένου στοιχείου. και το μέγεθός τους δεν επιτρέπεται να υπερβαίνει το αντίστοιχο μέγεθος έξι (6) απλών γραμμών κειμένου.

Σημ.
Η απαίτηση αυτή (για την αναφορά της ύπαρξης γραφικού ή εικόνας σε κάποιο σημείο του δελτίου του στοιχείου με την ένδειξη «[Εικόνα]»*), θα μπορούσε και να παραληφθεί αφού δεν προσφέρει καμία πληροφόρηση για το περιεχόμενο του γραφικού ή της εικόνας, αλλά αποτελεί μια ελάχιστη ένδειξη, περί της ύπαρξής τους ή όχι.*
Εναλλακτικά, για την αποφυγή πιθανών συγχύσεων στην εμφάνιση και τη μορφή των στοιχείων, αλλά και για λόγους απλοποίησης και ομοιομορφίας, θα μπορούσε ακόμη και να μην επιτρέπεται καθόλου η χρήση γραφικών ή εικόνων στα εκδιδόμενα δελτία των στοιχείων.

5.4. Δημιουργία ΠΑΗΨΣ

5.4.1. Για την δημιουργία της ΠΑΗΨΣ, αποστέλλονται στην ΕΑΦΔΣΣ όλα ανεξαιρέτως τα σύμβολα και οι χαρακτήρες που είναι εκτυπώσιμοι στο δελτίο του στοιχείου, ώστε να υπάρχει ταύτιση χαρακτήρων και αριθμού γραμμών κειμένου. Για το σκοπό αυτό –όταν και όπου απαιτείται- αποστέλλονται επιπλέον και οι εξής κωδικοί χαρακτήρες και μόνον αυτοί :

- κενού χαρακτήρα – διαστήματος (space)
- στηλοθέτη (TAB)
- αλλαγής γραμμής (line feed - LF)
- αρχής νέας γραμμής (carriage return - CR)η
- αλλαγής σελίδας (next page – NP)
- τέλους αρχείου (end o f file - EOF)

5.4.2. Η ΕΑΦΔΣΣ αφού λάβει τα δεδομένα αυτά, προσθέτει άμεσα σε αυτά, χωρίς καμία άλλη ενδιάμεση παρεμβολή, μια συμβολοσειρά σταθερού μήκους 23 χαρακτήρων η οποία αποτελείται από:

- τον 11-ψήφιο αρ. Μητρώου της ΕΑΦΔΣΣ, ο οποίος σχηματίζεται από : 3 χαρακτήρες – γράμματα του αριθμού έγκρισης, και τα 8 ψηφία του εργοστασιακού σειριακού αριθμού παραγωγής της ΕΑΦΔΣΣ.
- τον γενικό αύξοντα αριθμό σήμανσης – έκδοσης στοιχείου σε μορφή μετρητή σταθερού μήκους 8 ψηφίων. Ο α/α αναγράφεται στο δεξιότερο μέρος και οι τυχόν υπόλοιπες θέσεις (μέχρι τον αριθμό 8) των ψηφίων συμπληρώνονται με 0. Δεν παρεμβάλλεται κανένα σύμβολο διαχωρισμού τριάδων (εκατοντάδων, χιλιάδων κλπ).
- τον ημερήσιο αύξοντα αριθμό σήμανσης – έκδοσης στοιχείου σε μορφή μετρητή σταθερού μήκους 4 ψηφίων. Ο α/α αναγράφεται στο δεξιότερο μέρος και οι τυχόν υπόλοιπες θέσεις (μέχρι τον αριθμό 4) των ψηφίων συμπληρώνονται με 0. Δεν παρεμβάλλεται κανένα σύμβολο διαχωρισμού τριάδων (εκατοντάδων, χιλιάδων κλπ).

5.4.3. Τα δεδομένα αυτά επεξεργάζονται από την ΕΑΦΔΣΣ μέσω του ειδικού ασφαλούς αλγορίθμου SHA-1, και από το αποτέλεσμα της επεξεργασίας προκύπτει η ΠΑΗΨΣ, του συγκεκριμένου στοιχείου, η οποία και αποστέλλεται μαζί με τον ημερήσιο και γενικό α/α αρίθμησης σήμανσης στοιχείου και τον αρ. μητρώου της ΕΑΦΔΣΣ, στον διασυνδεόμενο Η/Υ, για την αποτύπωση – εκτύπωσή στο υπό έκδοση στοιχείο και την δημιουργία και αποθήκευση του αντίστοιχου ηλεκτρονικού αρχείου της ΠΑΗΨΣ.

5.5. Αποτύπωση – εκτύπωση ΠΑΗΨΣ στο εκδιδόμενο στοιχείο – Συμβολοσειρά Σήμανσης Στοιχείου.

5.5.1. Η αποτύπωση – εκτύπωση της ΠΑΗΨΣ στο εκδιδόμενο από τον διασυνδεόμενο Η/Υ στοιχείο, γίνεται από το λογισμικό υποστήριξης της ΕΑΦΔΣΣ, το οποίο αφού λάβει τα προαναφερθέντα δεδομένα, ενσωματώνει στο προς εκτύπωση δελτίο του στοιχείου, την συμβολοσειρά της Σήμανσης του στοιχείου.

5.5.2. Η ενσωμάτωση της συμβολοσειράς της Σήμανσης του στοιχείου εντός του περιεχομένου του στοιχείου και αποτελεί πλέον μέρος του. Συγκεκριμένα η τοποθέτηση της συμβολοσειράς Σήμανσης, γίνεται στην αμέσως επόμενη εκτυπώσιμη γραμμή από αυτήν των τελευταία εκτυπώσιμων δεδομένων του στοιχείου, είναι σταθερού μήκους και περιλαμβάνει ακριβώς τους ίδιους 67 χαρακτήρες, οι οποίοι αποθηκεύονται και στο αντίστοιχο αρχείο της ΠΑΗΨΣ στον Η/Υ. Συγκεκριμένα η συμβολοσειρά Σήμανσης στοιχείου σχηματίζεται από :

- την αλληλουχία των 40 δεκαεξαδικών ΕΛΟΤ-928 χαρακτήρων της αντίστοιχης ΠΑΗΨΣ του στοιχείου (γίνεται χρήση μόνον αριθμών και κεφαλαίων λατινικών χαρακτήρων A…F).
- έναν κενό χαρακτήρα (διάστημα - space)
- τον ημερήσιο αύξοντα αριθμό σήμανσης – έκδοσης στοιχείου σε μορφή μετρητή σταθερού μήκους 4 ψηφίων. Ο α/α αναγράφεται στο δεξιότερο μέρος και οι τυχόν υπόλοιπες θέσεις (μέχρι τον αριθμό 4) των ψηφίων συμπληρώνονται με 0. Δεν παρεμβάλλεται κανένα σύμβολο διαχωρισμού τριάδων (εκατοντάδων, χιλιάδων κλπ).
- έναν κενό χαρακτήρα (διάστημα - space)

- τον γενικό α/α σήμανσης – έκδοσης στοιχείου σε μορφή μετρητή σταθερού μήκους 8 ψηφίων. Ο α/α αναγράφεται στο δεξιότερο μέρος και οι τυχόν υπόλοιπες θέσεις (μέχρι τον αριθμό 8) των ψηφίων συμπληρώνονται με 0. Δεν παρεμβάλλεται κανένα σύμβολο διαχωρισμού τριάδων (εκατοντάδων, χιλιάδων κλπ).
- έναν κενό χαρακτήρα (διάστημα - space)
- τον αρ. μητρώου της ΕΑΦΔΣΣ : (3 χαρακτήρες – γράμματα του αριθμού έγκρισης, ένας κενός χαρακτήρας (διάστημα - space), και ο α/α εργοστασιακός σειριακός αριθμός παραγωγής ο οποίος επίσης είναι σταθερού μεγέθους και σχηματίζεται από 8 ψηφία).

6. Τεχνικά Χαρακτηριστικά

6.1. Ειδικές Περιπτώσεις

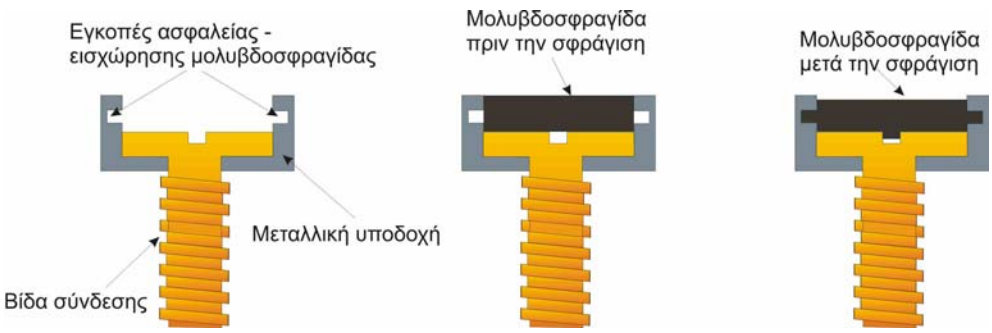
6.1.1. Οποιοδήποτε ζήτημα σχετίζεται με τις εφαρμογές ΕΑΦΔΣΣ, την εξειδίκευσή τους σε ειδικές περιπτώσεις και δεν αναφέρεται πλήρως στις παρούσες οδηγίες, εξετάζεται ειδικά από την αρμόδια διακομματική Επιτροπή του άρθρου 7 του ν. 1809/1988, η οποία και αποφασίζει σχετικά, λαμβάνοντας υπ' όψη όπου είναι δυνατό, τις σχετικές διατάξεις τού ιδίου νόμου καθώς και τα ισχύοντα σε αντίστοιχα σημεία των Τεχνικών Προδιαγραφών περί Φορολογικών Ταμειακών Μηχανών – Φορολογικών Μηχανισμών.

6.2. Θέση και Σφράγιση

6.2.1. Η πρόσβαση στο εσωτερικό της ΕΑΦΔΣΣ προστατεύεται από ειδική βίδα η οποία συνδέει το επάνω τμήμα της ΕΑΦΔΣΣ με την βάση της κατά τέτοιο τρόπο ώστε να είναι αδύνατη η πρόσβαση στο εσωτερικό της ΕΑΦΔΣΣ, χωρίς την αφαίρεσή της.

6.2.2. Η βίδα σφραγίζεται με σφραγίδα η οποία φέρει ειδικό κωδικό αριθμό του εξουσιοδοτημένου τεχνικού αντιπροσώπου. Ο αριθμός αυτός υποχρεωτικά περιλαμβάνει και τα χαρακτηριστικά γράμματα του αριθμού έγκρισης καταλληλότητας και είναι ίδιος με αυτόν που έχει κατατεθεί στο τμήμα Φορολογικών Ταμειακών Μηχανών και Συστημάτων, της Διεύθυνσης ΚΒΣ του Υπουργείου Οικονομίας και Οικονομικών.

6.2.3. Για την σφράγιση χρησιμοποιείται κατάλληλο υλικό (πχ μολυβδοσφραγίδα), το οποίο δεν επιδέχεται ξέσματα και γίνεται κατά τρόπο με τον οποίο είναι αδύνατη η αφαίρεσή της σφραγίδας, χωρίς την καταστροφή της.



6.2.4. Κατά την επανασφράγιση, πρέπει να δίδεται η απαραίτητη προσοχή, ώστε να είναι ευκρινής η αποτύπωση του α/α – ειδικού κωδικού αριθμού (του «ζουμπά»), του εξουσιοδοτημένου τεχνικού αντιπροσώπου.

6.2.5. Ο κάτοχος της άδειας είναι υπεύθυνος για την εφαρμογή του περιγραφέντος τρόπου σφράγισης και το σημείο αυτό ελέγχεται ειδικά από την Επιτροπή και τα αρμόδια ελεγκτικά όργανα.

6.3. Ηλεκτρική Τροφοδοσία

6.3.1. Οι ΕΑΦΔΣΣ διαθέτουν αυτόνομη είσοδο παροχής τροφοδοσίας ηλεκτρικού ρεύματος, είτε εναλλασσομένου (Τάσεως 230V ± 10%.συχνότητος 50Hz ± 5%.), είτε συνεχούς (12 ή 24 V DC).

6.3.2. Ενδεχόμενη εξωτερική ηλεκτρική τροφοδοτική διάταξη (ανορθωτής – μετασχηματιστής κλπ), θεωρείται αναπόσπαστο τμήμα της ΕΑΦΔΣΣ και της έγκρισής της.

6.3.4. Σε κατάσταση λειτουργίας σε σύνδεση με διασυνδεόμενο σύστημα Η/Υ, η ηλεκτρική τροφοδοσία της ΕΑΦΔΣΣ, είναι δυνατόν να λαμβάνεται από τον διασυνδεόμενο Η/Υ.

6.4. Πρόσθετα εξωτερικά χειριστήρια

6.4.1. Η ΕΑΦΔΣΣ διαθέτει την ελάχιστη αναγκαία δυνατότητα εξωτερικών χειρισμών, έτσι ώστε να είναι δυνατή η έκδοση δελτίων απαραίτητων στοιχείων, σε αυτόνομη λειτουργία και κατάσταση αποσύνδεσης από το διασυνδεδεμένο σύστημα Η/Υ. Τέτοια απαραίτητα στοιχεία είναι:
α) η έκδοση του Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Ζ»,
β) η έκδοση Δελτίου Συνόψεων - Υπογραφών Ημέρας - (ΔΣΥΜ).
γ) η έκδοση του Δελτίου Ανάγνωσης Περιόδου Φορολογικής Μνήμης Ημερήσιων Συνόψεων – (ΔΑΠΦΜΗΣ), με δυνατότητα επιλογής ημερολογιακής περιόδου και περιόδου από α/α «Ζ» έως α/α «Ζ».

6.4.2. Οι χειρισμοί αυτοί είναι δυνατόν να γίνονται μέσω ειδικών πλήκτρων, κλειδιού ή συνδυασμού αυτών. Ενδεχόμενο αποσπώμενο χειριστήριο για την έκδοση των παραπάνω στοιχείων, θεωρείται αναπόσπαστο τμήμα της ΕΑΦΔΣΣ και της έγκρισής της.

6.4.3. Το χειριστήριο αυτό ή το σημείο σύνδεσής του, στην περίπτωση που αυτό είναι αποσπώμενο, είναι δυνατόν να προστατεύεται, από τυχόν βανδαλισμούς ή άσκοπη χρήση.

6.4.4. Η ΕΑΦΔΣΣ είναι δυνατόν να διαθέτει και άλλες επιπλέον θύρες, οι οποίες όμως είναι αποκλειστικά για την προσθήκη χειριστηρίων όπως πληκτρολογίων και οθονών χειρισμού περισσοτέρων δυνατοτήτων προγραμματισμού, δηλώσεων, ρυθμίσεων, τεχνικού ελέγχου και άλλων διαλόγων χειρισμών.

6.5. Διασύνδεση - Επικοινωνία Δεδομένων

6.5.1. Η σύνδεση της ΕΑΦΔΣΣ με σύστημα διασυνδεόμενου Η/Υ, μέσω της ΕΘΕΔ, δύναται να είναι ενσύρματη ή ασύρματη :

6.5.1.1. **Ενσύρματη** (μέσω αγώγιμων μεταλλικών επαφών) :
α) είτε απευθείας χωρίς την παρεμβολή καλωδίων (βύσμα με βύσμα),
β) είτε καλωδιακά.

6.5.1.2. **Ασύρματη**

6.5.2. Στην περίπτωση καλωδιακής σύνδεσης,

6.5.2.1. Στην ΕΘΕΔ συνδέεται μόνον ένα καλώδιο πολλαπλών δυνατοτήτων, (πολύκλωνο ή άλλο), συνεχόμενο, μη διακοπτόμενο και μη συνδεόμενο καλωδιακά ή αλλιώς με άλλες παρεμβαλλόμενες συσκευές.

6.5.2.2. Προσδιορίζεται ρητά από τον κατασκευαστή το είδος του καλωδίου σύνδεσης καθώς και το μήκος της απρόσκοπτης και λειτουργικής επικοινωνίας Η/Υ – της ΕΑΦΔΣΣ.

6.5.2.3. Το καλώδιο θα πρέπει να φέρει θωράκιση σε παρεμβολές ηλεκτρομαγνητικών θορύβων και να έχει ηλεκτρομαγνητική ατρωσία.

6.5.2.4. Το καλώδιο σύνδεσης αποτελεί αναπόσπαστο τμήμα της ΕΑΦΔΣΣ και της έγκρισής της.

6.5.3. Στην περίπτωση ασύρματης διασύνδεσης, εάν αυτό είναι απαραίτητο, απαιτείται άδεια χρήσης συχνοτήτων από τους αρμόδιους κρατικούς φορείς.

6.5.4. Η πλήρης περιγραφή, οι συνθήκες και το περιβάλλον του τρόπου διασύνδεσης, καθώς και το πρωτόκολλο επικοινωνίας, κατατίθενται αναλυτικά στην επιτροπή.

6.6. Μπαταρία Ρολογιού και CMOS – RAM

6.6.1. Η ΕΑΦΔΣΣ είναι εφοδιασμένη με ειδικό κύκλωμα ελέγχου της κατάστασης της μπαταρίας της CMOS – RAM και του ρολογιού της ΕΑΦΔΣΣ. Σε περίπτωση πτώσης τάσης της μπαταρίας, κάτω του δηλουμένου από τον κατασκευαστή επιπέδου, ή σε περίπτωση μη υπάρξεως σχετικής δηλώσεως, κάτω του 90% της ονομαστικής τιμής της, τούτο σηματοδοτείται στην οθόνη και καταγράφεται σχετικό μήνυμα στον εκτυπωτή.

6.6.2. Γενικά η ΕΑΦΔΣΣ δεν επιτρέπει καμία συναλλαγή, εάν δεν υπάρχει ικανή τροφοδοσία από την μπαταρία της μνήμης εργασίας.

6.7. Σκόπιμος μηδενισμός της μνήμης εργασίας μέσω βραχυκυκλωτήρα

6.7.1. Η ΕΑΦΔΣΣ είναι εφοδιασμένη με ειδικό κύκλωμα ελέγχου ή και το κατάλληλο λογισμικό, το οποίο έχει την δυνατότητα να ανιχνεύει την βραχυκύκλωση των ακροδεκτών τροφοδοσίας της μνήμης εργασίας - μπαταρίας (παραμονή βραχυκυκλωτήρα).

6.7.2. Η περίπτωση αυτή σηματοδοτείται με ηχητικό σήμα ή και εκτύπωση χαρακτηριστικού μηνύματος, και σηματοδοτεί το γεγονός, ότι πλέον δεν είναι δυνατή καμία λειτουργία δημιουργίας ΠΑΗΨΣ ή έκδοσης ΕΦΔ, μέχρι να αρθεί η κατάσταση αυτή.

6.8. Μνήμη προγραμμάτων.

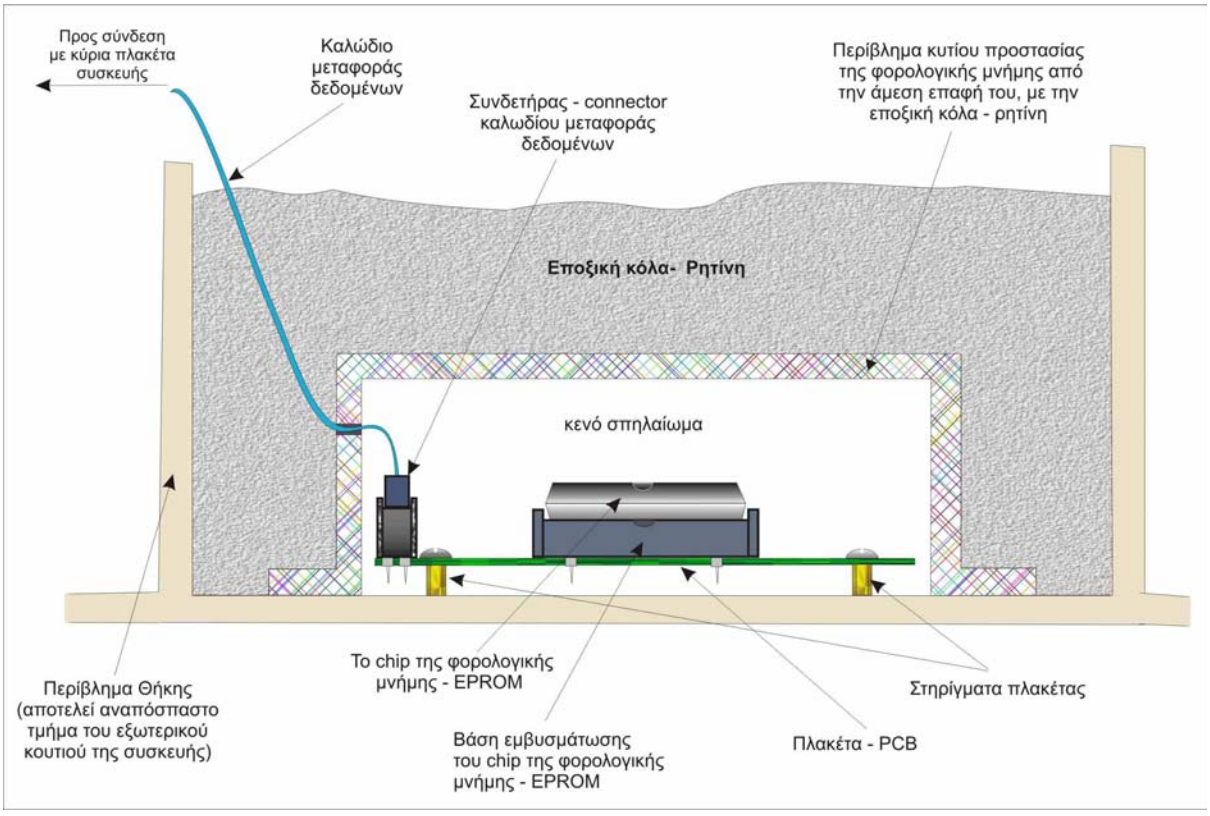
6.8.1. Η μνήμη προγραμμάτων είναι μνήμη ημιαγωγών αποκλειστικά ανάγνωσης. Επιτρέπεται η χρήση μόνο καινούργιων μνημών.

6.8.2. Η υλοποίηση της κατασκευής της ΕΑΦΔΣΣ δεν επιτρέπει με κανένα τρόπο τυχόν αλλαγές του ενταμιευμένου στη μνήμη προγραμμάτων λογισμικού, χωρίς την αποσφράγιση της ΕΑΦΔΣΣ. Για κάθε αλλαγή – τροποποίηση του λογισμικού ή του υλικού μέρους της ΕΑΦΔΣΣ, κατατίθεται αίτηση στην Επιτροπή η οποία και αποφασίζει σχετικά.

6.9. Ασφάλεια Φορολογικής Μνήμης

6.9.1. Τα κυκλώματα της φορολογικής μνήμης, προστατεύονται σε ειδικό κυτίο, το οποίο τοποθετείται σε ειδικά διαμορφωμένη υποδοχή που αποτελεί αναπόσπαστο τμήμα του περιβλήματος της ΕΑΦΔΣΣ. Η θήκη με το κυτίο της φορολογικής μνήμης πακτώνεται και σφραγίζεται με ειδικό υλικό (εποξική ρητίνη) με τέτοιο τρόπο ώστε να είναι αδύνατη η αφαίρεση του κυτίου της φορολογικής μνήμης, χωρίς την καταστροφή του περιβλήματος της ΕΑΦΔΣΣ.

Σχηματικό Παράδειγμα Σφράγισης της Φορολογικής Μνήμης



6.9.2. Το περιεχόμενο της φορολογικής μνήμης διατηρείται αναλλοίωτο χωρίς χρονικό περιορισμό και υπό όλες τις συνθήκες. Τα δεδομένα της φορολογικής μνήμης που τυχόν εμφανίσει βλάβη και αντικατασταθεί, είναι αναγνώσιμα από ειδική συσκευή για χρήση από τις φορολογικές υπηρεσίες, με εξαίρεση τις περιπτώσεις αδύνατης τεχνικά ανάγνωσης. Η περίπτωση αυτή τεκμηριώνεται πλήρως από τεχνική έκθεση – αναφορά του κατέχοντος την άδεια καταλληλότητας, η οποία με ευθύνη του, αποστέλλεται άμεσα, στην Επιτροπή, ενώ αντίγραφό της επισυνάπτεται στο Πρωτόκολλο αφαίρεσης της φορολογικής μνήμης και κατατίθεται στην αρμόδια ΔΟΥ του κατόχου της ΕΑΦΔΣΣ.

7. Λειτουργικά Χαρακτηριστικά

7.1. Κύριες Λειτουργίες – Βασικά Χαρακτηριστικά

7.1.1. Τα Βασικά Λειτουργικά Χαρακτηριστικά της ΕΑΦΔΣΣ είναι :

- Επικοινωνεί με διασυνδεόμενο Η/Υ για λήψη δημοσιονομικών δεδομένων για κάθε έκδοση στοιχείου που χειρίζεται ο Η/Υ.
- Επεξεργάζεται τα δεδομένα αυτά και δημιουργεί μέσω του ειδικού Ασφαλούς Αλγορίθμου SHA-1, μια μονοσήμαντη ΠΑΗΨΣ, για κάθε ένα εκδιδόμενο στοιχείο.
- Αριθμεί και διαφυλάσσει στη μνήμη εργασίας κάθε δημιουργούμενη ΠΑΗΨΣ.
- Εκδίδει το σχετικό ΔΦΣΣ.
- Αποστέλλει για κάθε δημιουργηθείσα ΠΑΗΨΣ, την ίδια την ΠΑΗΨΣ, την αρίθμησή της, τον αρ. Μητρώου ΕΑΦΔΣΣ, καθώς και οποιοδήποτε απαιτούμενο στοιχείο, στον διασυνδεόμενο Η/Υ.
- Με την ημερήσια διαδικασία έκδοσης του ΔΗΦΑΣΣ - «Ζ», δημιουργεί, μέσω του ειδικού Ασφαλούς Αλγορίθμου SHA-1, την μονοσήμαντη γενική ΠΑΗΨΣ όλων των ΠΑΗΨΣ της ημέρας και την αποθηκεύει μόνιμα στη Φορολογική Μνήμη, μαζί με όλα τα λοιπά απαραίτητα στοιχεία (ημερήσιος αριθμός ΠΑΗΨΣ, κλπ).
- Αποστέλλει την δημιουργηθείσα γενική ημερήσια ΠΑΗΨΣ και οποιοδήποτε απαιτούμενο στοιχείο, στον διασυνδεόμενο Η/Υ.
- Εκδίδει όλα τα απαραίτητα δελτία, όπως τα ΕΦΔ και τα λοιπά διαγνωστικά ή πληροφοριακά δελτία χειρισμών και προγραμματισμού.
- Ανιχνεύει οποιαδήποτε βλάβη της μνήμης εργασίας καθώς και κάθε περίπτωση αποσύνδεσης του διασυνδεόμενου Η/Υ, κατά την επικοινωνία της με αυτόν.

7.2. Αποσύνδεση

7.2.1. Ως αποσύνδεση της ΕΑΦΔΣΣ, θεωρείται κάθε αδυναμία αποστολής και λήψης δεδομένων μεταξύ αυτής και του λογισμικού συνεργασίας του διασυνδεόμενου Η/Υ.

7.2.2. Σε περίπτωση ανίχνευσης αποσύνδεσης, κάθε λειτουργία σήμανσης, αποθήκευσης σύνοψης και έκδοσης δελτίων από την ΕΑΦΔΣΣ είναι αδύνατη.

7.2.3. Η αποσύνδεση γίνεται αντιληπτή από το λογισμικό υποστήριξης της ΕΑΦΔΣΣ στον διασυνδεόμενο Η/Υ, σε κάθε προσπάθεια επικοινωνίας του με την ΕΑΦΔΣΣ, και με κατάλληλο μήνυμα, προειδοποιεί το χειριστή του Η/Υ για το γεγονός αυτό. Στην περίπτωση που η αποσύνδεση έγινε μετά την έναρξη της διαδικασίας αποστολής δεδομένων για την δημιουργία ΠΑΗΨΣ και προ της λήψής της, τότε η διαδικασία αυτή ακυρώνεται, ως μη γενομένη, και επαναλαμβάνεται μετά την ανίχνευση της επανασύνδεσης.

7.2.4. Ο μέγιστος χρόνος ανίχνευσης της αποσύνδεσης, δεν μπορεί να υπερβαίνει τα 30 δευτερόλεπτα.

7.2.5. Στην περίπτωση αποσύνδεσης της ΕΑΦΔΣΣ από το διασυνδεόμενο σύστημα, όταν αυτό ευρίσκεται σε κατάσταση αποστολής ή λήψης δεδομένων :

- Το γεγονός αριθμείται ως Α/Α αποσυνδέσεων στη μνήμη εργασίας.
- Αυτόματα η ΕΑΦΔΣΣ σηματοδοτείται ανάλογα, με την εκτύπωση σχετικού μηνύματος Παράνομης Απόδειξης «Αποσύνδεση ΕΘΕΔ # xxx Ημερομηνία : ηη/μμ/εε Ώρα : ωω:λλ». Η εκτύπωση αυτή συνοδεύεται από σχετικό χαρακτηριστικό ηχητικό σήμα και εφόσον δεν έχει μεσολαβήσει διακοπή ηλεκτρικής τροφοδοσίας ή αποκατάσταση της αποσύνδεσης (επανασύνδεση), επαναλαμβάνεται τουλάχιστον 10 φορές, πέραν των οποίων είναι δυνατόν η ΕΑΦΔΣΣ, αυτομάτως να διακόπτει την λειτουργία της.
- Στην περίπτωση που η αποσύνδεση συμβεί πριν, κατά ή μετά την διαδικασία δημιουργίας ΠΑΗΨΣ, μετά από λήψη σχετικών δεδομένων, τότε ακυρώνεται η διαδικασία αυτή και διαγράφεται η τυχόν δημιουργηθείσα ΠΑΗΨΣ, από τη μνήμη εργασίας της ΕΑΦΔΣΣ.

7.2.6. Ο α/α αποσυνδέσεων # xxx εγγράφεται στη Φορολογική Μνήμη, με την έκδοση του Δελτίου Ημερήσιας Αναφοράς Σήμανσης Στοιχείων - «Z», σε ιδιαίτερο αθροιστή Αποσυνδέσεων ΕΘΕΔ. Ο αριθμός αυτών των αποσυνδέσεων, είναι συνεχής, προοδευτικός και εμφανίζεται σε κάθε Δελτίο Ημερήσιας Αναφοράς Σήμανσης Στοιχείων - «Z».

7.3. Ασφάλεια δεδομένων ΕΑΦΔΣΣ

7.3.1. Η ΕΑΦΔΣΣ δεν επικοινωνεί με τον διασυνδεόμενο Η/Υ (δεν δέχεται ούτε αποστέλλει δεδομένα) από άλλη θύρα εκτός της ΕΘΕΔ. Εάν η ΕΑΦΔΣΣ διαθέτει κανονικό ή περιορισμένων δυνατοτήτων πληκτρολόγιο – χειριστήριο (ενσωματωμένο ή αποσπόμενο), τότε αυτό θα χρησιμοποιείται αποκλειστικά και μόνο για χειρισμούς προγραμματισμού και δηλώσεων παραμέτρων της ΕΑΦΔΣΣ. Η ΕΑΦΔΣΣ είναι εφοδιασμένη εξ αρχής με ειδικό λογισμικό που δεν επιτρέπει έκδοση δελτίων κατευθείαν από το πληκτρολόγιο, ή την εισαγωγή δεδομένων για έκδοση δελτίων από άλλη θύρα ή με άλλο τρόπο πέραν της ΕΘΕΔ.

7.3.2. Τα στοιχεία από κάθε εκδοθέν δελτίο, σωρεύονται σε αντίστοιχους σωρευτές στη μνήμη εργασίας της ΕΑΦΔΣΣ. Το λογισμικό της ΕΑΦΔΣΣ προστατεύει με ειδικό σύστημα ασφάλειας το περιεχόμενο της μνήμης εργασίας και δεν επιτρέπει με κανένα τρόπο την ακύρωση / διαγραφή, η αφαίρεση αριθμών από τους ημερήσιους σωρευτές / αθροιστές της μνήμης εργασίας, εκτός μόνον της περιπτώσεως μη ολοκληρώσεως της διαδικασίας λήψης δεδομένων, δημιουργίας και αποστολής ΠΑΗΨΣ, λόγω αποσυνδέσεως .

7.3.3. Το λογισμικό της ΕΑΦΔΣΣ δεν επιτρέπει την εγγραφή αρνητικών αριθμών στην Φορολογική Μνήμη.

7.3.4. Ο μηδενισμός μνήμης εργασίας γίνεται μόνον μετά την επιτυχή μεταφορά και εγγραφή των απαραίτητων στοιχείων στη φορολογική μνήμη. Τα δεδομένα που εγγράφονται στην φορολογική μνήμη και εκτυπώνονται στο δελτίο ΔΗΦΑΣΣ – «Z»

προέρχονται αποκλειστικά και μόνο από αυτά που έχουν διαμορφωθεί και συσσωρευτεί στη μνήμη εργασίας. Το λογισμικό της ΕΑΦΔΣΣ δεν επιτρέπει με κανένα τρόπο την έκδοση του δελτίου ΔΗΦΑΣΣ – «Z» κατευθείαν, από δεδομένα που έχουν προσχηματισθεί σε διασυνδεόμενο σύστημα Η/Υ και προέρχονται κατ' ευθείαν απ' αυτό.

7.4. Βλάβη Μνήμης Εργασίας (CMOS Error)

7.4.1. Η ΕΑΦΔΣΣ διαθέτει κατάλληλα ηλεκτρονικά κυκλώματα ή και λογισμικό, για την ανίχνευση, αρίθμηση και καταγραφή οποιασδήποτε βλάβης της μνήμης εργασίας (CMOS Error).

7.4.2. Η διαπίστωση της βλάβης της μνήμης εργασίας σηματοδοτείται από την ΕΑΦΔΣΣ, με σχετικό προειδοποιητικό ηχητικό σήμα, ή και την εκτύπωση αντίστοιχου ενδεικτικού μηνύματος.

7.4.3. Πέραν αυτού, τα ηλεκτρονικά κυκλώματα και το λογισμικό της ΕΑΦΔΣΣ, δεν επιτρέπουν καμία λειτουργία της ΕΑΦΔΣΣ, πριν από την αποκατάσταση της βλάβης.

7.4.4. Η βλάβη της μνήμης εργασίας γίνεται αντιληπτή από το λογισμικό υποστήριξης του διασυνδεόμενου Η/Υ, σε κάθε προσπάθεια επικοινωνίας του με την ΕΑΦΔΣΣ, και με κατάλληλο μήνυμα, προειδοποιεί το χειριστή του Η/Υ για το γεγονός αυτό.

7.4.5. Μετά από κάθε ανίχνευση βλάβης της μνήμης εργασίας :

- Η βλάβη, αφού ανιχνευθεί από τα κυκλώματα της ΕΑΦΔΣΣ, αποκαθίσταται από εξουσιοδοτημένο τεχνικό και καταγράφεται στο συνοδευτικό βιβλιάριο συντήρησης.
- Ενεργοποιείται με ευθύνη του κατόχου - χειριστή της ΕΑΦΔΣΣ, το λογισμικό υποστήριξης της ΕΑΦΔΣΣ, που ευρίσκεται στο διασυνδεόμενο Η/Υ.
- Αποστέλλονται εκ νέου στην ΕΑΦΔΣΣ τα δεδομένα όλων των φορολογικών στοιχείων, ένα – ένα, με την σειρά που εκδόθηκαν – «σημάνθηκαν» προ της εμφανίσεως της βλάβης της μνήμης εργασίας για την εκ νέου δημιουργία των απαραίτητων συνόψεων (ΠΑΗΨΣ) και λοιπών δημοσιονομικών δεδομένων (αθροιστών κλπ), τα οποία είναι απαραίτητα για την δημιουργία της γενικής ημερήσιας «σύνοψης – υπογραφής».
- Στην περίπτωση αυτή δεν αποστέλλεται προς τον διασυνδεόμενο Η/Υ, κανένα στοιχείο, από την ΠΑΗΨΣ, την αρίθμησή της ή τον αρ. μητρώου της ΕΑΦΔΣΣ.
- Στα εκ νέου εκδιδόμενα ΔΦΣΣ, υποχρεωτικά αναγράφεται η χαρακτηριστική ένδειξη «ΕΠΑΝΑΛΗΨΗ»
- Εκδίδεται το σχετικό Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z».

7.4.6. Υποχρεωτικά το λογισμικό της ΕΑΦΔΣΣ έχει δυνατότητα χειρισμού τουλάχιστον τριψήφιου αριθμού βλαβών CMOS (μπορεί δηλαδή να αριθμήσει τουλάχιστον 1000 βλάβες CMOS). Η αρίθμηση γίνεται υποχρεωτικά στο δεκαδικό αριθμητικό σύστημα και δεν επιτρέπεται αποτύπωση σε άλλο αριθμητικό σύστημα πχ σε δεκαεξαδική αρίθμηση (9, A, B, C, …κλπ).

7.5. Ειδικές περιπτώσεις έκδοσης Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z»

7.5.1. Δυνατότητα έκδοσης «μηδενικού» Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z»

7.5.1.1. Η δυνατότητα έκδοσης του Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z» είναι υποχρεωτική ακόμη και στην περίπτωση κατά την οποία δεν έχει μεσολαβήσει η έκδοση κανενός Δελτίου Φορολογικής Σήμανσης Στοιχείου (ΔΦΣΣ) από την αμέσως προηγούμενη (τελευταία) έκδοση Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z».

7.5.1.2. Στην περίπτωση αυτή, στο Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) – «Z» αναγράφονται :

- ημερομηνία και ώρα έκδοσης του δελτίου
- ο γενικός α/α (από αρχής λειτουργίας της ΕΑΦΔΣΣ) του εκδιδόμενου Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων - «Z»
- Η χαρακτηριστική ένδειξη «Δεν έχει μεσολαβήσει η έκδοση κανενός Δελτίου Φορολογικής Σήμανσης Στοιχείου (ΔΦΣΣ) από την αμέσως προηγούμενη (τελευταία) έκδοση Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - Z».
- Η χαρακτηριστική ένδειξη «Συνολικός Αριθμός Εκδοθέντων Δελτίων Φορολογικής Σήμανσης Στοιχείων» μαζί με τον γενικό α/α (από αρχής λειτουργίας της ΕΑΦΔΣΣ) του τελευταία εκδοθέντος Δελτίου Φορολογικής Σήμανσης Στοιχείου.
- Ο Ημερήσιος και ο Γενικός (από αρχής λειτουργίας της ΕΑΦΔΣΣ) α/α αριθμός Αποσυνδέσεων της ΕΑΦΔΣΣ.
- Ο Ημερήσιος και ο Γενικός (από αρχής λειτουργίας της ΕΑΦΔΣΣ) α/α αριθμός Βλαβών Μνήμης Εργασίας (CMOS-Error).

7.5.1.3. Πριν την έκδοση «μηδενικού» Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) «Z», η ΕΑΦΔΣΣ ειδοποιεί σχετικά το χειριστή για το γεγονός αυτό, ο οποίος με κατάλληλο χειρισμό (π.χ. πληκτρολόγηση) επιβεβαιώνει την διεκπεραίωση ή την ακύρωση της έκδοσης του δελτίου αυτού.

7.5.2. Υποχρεωτική η έκδοση Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z», μετά την παρέλευση 24 ωρών από το αμέσως προηγούμενο αντίστοιχο δελτίο.

7.5.2.1. Η έκδοση του Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z», είναι υποχρεωτική στην περίπτωση κατά την οποία έχουν παρέλθει 24 ώρες από την αμέσως προηγούμενη (τελευταία), έκδοση Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z» και στο χρονικό αυτό διάστημα έχει μεσολαβήσει η έκδοση, τουλάχιστον ενός Δελτίου Φορολογικής Σήμανσης Στοιχείου (ΔΦΣΣ).
7.5.2.2. Η περίπτωση αυτή ανιχνεύεται και ελέγχεται από το λογισμικό της ΕΑΦΔΣΣ, και σε περίπτωση διαπίστωσης :

- Η ΕΑΦΔΣΣ σηματοδοτεί κατάλληλα τον χειριστή με σχετικό προειδοποιητικό ηχητικό σήμα, ή και την εκτύπωση αντίστοιχου ενδεικτικού μηνύματος.
- Τα ηλεκτρονικά κυκλώματα και το λογισμικό της ΕΑΦΔΣΣ, δεν επιτρέπουν καμία λειτουργία της ΕΑΦΔΣΣ, εκτός από την έκδοση Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z».
- Η ΕΑΦΔΣΣ υποχρεωτικά εκδίδει Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων – (ΔΗΦΑΣΣ) - «Z».

7.5.3. **Διακοπή Ηλεκτρ. Τροφοδοσίας κατά την έκδοση Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων – (ΔΗΦΑΣΣ) - «Z»**

7.5.3.1. Το λογισμικό της ΕΑΦΔΣΣ κατά την διάρκεια έκδοσης του Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων – (ΔΗΦΑΣΣ) - «Z», έχει τη δυνατότητα αναγνώρισης και διαχείρισης της διακοπής ηλεκτρικής τροφοδοσίας, ως εξής :

α) μετά την επαναφορά της ηλεκτρικής τροφοδοσίας, ενημερώνεται ο χειριστής ότι δεν ολοκληρώθηκε επιτυχώς η έκδοση του Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων – (ΔΗΦΑΣΣ) - «Z» με ανάλογη ηχητική ένδειξη και εκτύπωση σχετικού μηνύματος «ΔΙΑΚΟΠΗ ΡΕΥΜΑΤΟΣ – ΑΝΕΠΙΤΥΧΗΣ ΕΚΔΟΣΗ Z – ΠΑΡΑΝΟΜΗ ΑΠΟΔΕΙΞΗ - ΔΙΩΚΕΤΑΙ ΑΠΟ ΤΟ ΝΟΜΟ».

β) εάν η διακοπή της ηλεκτρικής τροφοδοσίας συνέβη μετά από επιτυχή ενταμίευση των δεδομένων στη Φορολογική Μνήμη, τότε η ΕΑΦΔΣΣ υποχρεωτικά εκτυπώνει το Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων – (ΔΗΦΑΣΣ) - «Z», χωρίς να εκτελείται ξανά ενταμίευση δεδομένων στη φορολογική μνήμη. Στην περίπτωση αυτή το λογισμικό της ΕΑΦΔΣΣ απαγορεύει την έκδοση οποιουδήποτε Ειδικού Φορολογικού Δελτίου, πριν την επιτυχή ολοκλήρωση της έκδοσης του Δελτίου «Z».

7.5.4. **Ανίχνευση τέλους χαρτιού κατά την έκδοση Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων – (ΔΗΦΑΣΣ) - «Z»**

7.5.4.1. Το λογισμικό της ΕΑΦΔΣΣ κατά την διάρκεια έκδοσης του Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων – (ΔΗΦΑΣΣ) - «Z», έχει τη δυνατότητα αναγνώρισης της ύπαρξης ή μη του χαρτιού στον εκτυπωτικό μηχανισμό. Στην περίπτωση ανίχνευσης μη ύπαρξης χαρτιού για την ολοκλήρωση της εκτύπωσης του Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων – (ΔΗΦΑΣΣ) - «Z»,ενημερώνεται ο χειριστής με σχετική ηχητική ένδειξη. Η ενταμίευση των δεδομένων στη φορολογική μνήμη είναι ανεξάρτητη του γεγονότος αυτού και εκτελείται κανονικά.

7.5.4.2. Μετά την επανατροφοδοσία με χαρτί του εκτυπωτικού μηχανισμού η ΕΑΦΔΣΣ υποχρεωτικά εκτυπώνει το πλήρες Δελτίο Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείων – (ΔΗΦΑΣΣ) - «Z», χωρίς να εκτελείται ξανά ενταμίευση δεδομένων στη φορολογική μνήμη. Στην περίπτωση αυτή το λογισμικό της ΕΑΦΔΣΣ απαγορεύει την έκδοση οποιουδήποτε Ειδικού Φορολογικού Δελτίου, πριν την επιτυχή ολοκλήρωση της έκδοσης του Δελτίου «Z».

7.6. Αλλαγή Λεκτικού Επωνυμίας Κατόχου

7.6.1. Η ΕΑΦΔΣΣ έχει δυνατότητα τουλάχιστον 5 πλήρων αλλαγών στοιχείων (λεκτικών) επωνυμίας κατόχου. Ο αριθμός αυτός αναφέρεται υποχρεωτικά και περιγράφεται εμφανώς στα εγχειρίδια οδηγιών χειρισμού και συντήρησης. Δεν επιτρέπεται η αλλαγή λεκτικού εάν προηγουμένως δεν έχει προηγηθεί η έκδοση Δελτίου Ημερήσιας Φορολογικής Αναφοράς Σήμανσης Στοιχείου – (ΔΗΦΑΣΣ) - «Z».

7.6.2. Επιπλέον για την αλλαγή λεκτικού, μετά την έκδοση του «Z» δεν θα πρέπει να έχει μεσολαβήσει καμιά έκδοση Δελτίου Φορολογικής Σήμανσης Στοιχείου (ΔΦΣΣ). Μετά από κάθε αλλαγή λεκτικού, η ΕΑΦΔΣΣ σηματοδοτεί κατάλληλα με εκτύπωση σχετικού μηνύματος για τον εναπομείναντα αριθμό αλλαγών λεκτικού, πχ «ΠΡΟΣΟΧΗ : Αλλαγές Λεκτικού που έχουν Απομείνει : 4»

7.7. Αριθμός Μητρώου ΕΑΦΔΣΣ

7.7.1. Είναι υποχρεωτική η αναγραφή του Αρ. Μητρώου σε όλα τα εκδιδόμενα από την ΕΑΦΔΣΣ δελτία (πχ «Παράνομες Αποδείξεις», διάφορες αναφορές πληροφοριών για χειρισμούς και προγραμματισμούς κλπ). Ο αριθμός αυτός ταυτίζεται απόλυτα με αυτόν που αναγράφεται στα Ειδικά Φορολογικά Δελτία (ΕΦΔ).

7.7.2. Η ΕΑΦΔΣΣ έχει δυνατότητα εκτύπωσης 3 θέσεων για τα χαρακτηριστικά γράμματα του αριθμού έγκρισης της άδειας καταλληλότητας.

7.8. Βλάβη Φορολογικής Μνήμης (Μνήμης Εφορίας)

7.8.1. Κάθε αποσύνδεση, ή βλάβη (εκτός της πλήρωσης μνήμης), σηματοδοτείται κατάλληλα με ηχητικό σήμα, ή και εκτύπωση σχετικού μηνύματος. Στην περίπτωση αυτή το λογισμικό της ΕΑΦΔΣΣ δεν επιτρέπει την εκτέλεση καμίας άλλης λειτουργίας.(Η ΕΑΦΔΣΣ θα πρέπει να «μπλοκάρει»).

7.8.2. Στην περίπτωση πλήρωσης της Φορολογικής Μνήμης η μοναδική λειτουργία που επιτρέπεται, αλλά και υποχρεωτικά πρέπει να εκτελεί η ΕΑΦΔΣΣ, είναι η έκδοση Δελτίου Ανάγνωσης Περιόδου Φορολογικής Μνήμης Ημερήσιων Συνόψεων – (ΔΑΠΦΜΗΣ).

7.8.3. Κάθε περίπτωση διαπίστωσης βλάβης φορολογικής μνήμης από τον κατέχοντα την άδεια καταλληλότητας ή της τεχνικής υποστήριξης ή από εξουσιοδοτημένο τεχνικό του αντιπρόσωπο, γνωστοποιείται άμεσα στην Επιτροπή.

7.8.4. Για το σκοπό αυτό ο κάτοχος της άδειας, συντάσσει, υπογράφει και αποστέλλει τεκμηριωμένη και λεπτομερή τεχνική αναφορά για το πρόβλημα μνήμης που διαπιστώθηκε, εντός 2 εργασίμων ημερών στην Επιτροπή. Ένα αντίγραφο της τεχνικής αναφοράς επισυνάπτεται στο συνοδευτικό βιβλιάριο συντήρησης (στο οποίο έχουν σημειωθεί και οι σχετικές αναφορές) από τον εξουσιοδοτημένο τεχνικό και ένα αντίγραφο αποστέλλεται στην αρμόδια ΔΟΥ του κατόχου της ΕΑΦΔΣΣ.

7.9. Έλεγχος ημερομηνίας ρολογιού της ΕΑΦΔΣΣ σε σχέση με το «Z».

7.9.1. Δεν επιτρέπεται η δυνατότητα διόρθωσης του ρολογιού (της ημερομηνίας) της ΕΑΦΔΣΣ, με ημερομηνία προγενέστερη εκείνης με την οποία καταγράφηκε στην φορολογική μνήμη και εκδόθηκε το τελευταίο «Z».

7.9.2. Το λογισμικό της ΕΑΦΔΣΣ είναι σε θέση να ελέγχει την τρέχουσα ημερομηνία του ρολογιού της μηχανής σε σχέση με αυτήν της τελευταίας έκδοσης του «Z». Η δυνατότητα αυτή ενεργοποιείται :

- 1ον κατά την ημερήσια έναρξη (Initialize) λειτουργίας της ΕΑΦΔΣΣ κατά την οποία να ελέγχεται η ημερομηνία του τελευταία εγγεγραμμένου «Z», με την τρέχουσα, και εάν υπάρχει διαφορά ημερομηνίας, ειδοποιείται σχετικά ο χειριστής ο οποίος είναι υπεύθυνος για την κλήση εξουσιοδοτημένου τεχνικού για την ρύθμιση της σωστής ημερομηνίας και ώρας.
- 2ον κατά την έναρξη της διαδικασίας έκδοσης του «Z», κατά την οποία ελέγχεται η ημερομηνία του τελευταίου εγγεγραμμένου «Z», με αυτήν της τρέχουσας (μ 'αυτήν που πάει να εκδοθεί το «Z»), και εάν υπάρχει διαφορά ημερομηνίας :

  α)εάν η τρέχουσα είναι μεγαλύτερη από την καταχωρημένη τελευταία : Ειδοποιείται ο χειριστής για την διαφορά αυτή και το μη αντιστρεπτό της διαδικασίας. Τέλος του ζητείται επιβεβαίωση με κατάλληλο χειρισμό για την έκδοση του δελτίου «Z».

  β)εάν η τρέχουσα ημερομηνία είναι μικρότερη από αυτήν της καταχώρησης του τελευταίου «Z» : ΔΕΝ ΕΠΙΤΡΕΠΕΤΑΙ Η ΕΚΔΟΣΗ ΤΟΥ ΔΕΛΤΙΟΥ «Z». Το γεγονός αυτό σηματοδοτείται κατάλληλα με σχετικό ηχητικό σήμα ή και αντίστοιχη εκτύπωση μηνύματος.

7.9.3. Ο χειριστής είναι υπεύθυνος για την κλήση εξουσιοδοτημένου τεχνικού για την ρύθμιση της σωστής ημερομηνίας και ώρας.

7.9.4. Κατά την διαδικασία αλλαγής της ημερομηνίας του ρολογιού της ΕΑΦΔΣΣ από εξουσιοδοτημένο τεχνικό ΔΕΝ ΕΠΙΤΡΕΠΕΤΑΙ η εισαγωγή ημερομηνίας μικρότερης από αυτήν του τελευταία εγγεγραμμένου «Z»,

7.9.5. Το λογισμικό της ΕΑΦΔΣΣ δεν επιτρέπει με κανένα τρόπο την εγγραφή στη φορολογική μνήμη, ημερομηνίας μικρότερης από αυτήν που έχει ενταμιευθεί το τελευταίο εγγεγραμμένο «Z».

7.10. Ασφάλεια Πρόσβασης - Καταγραφή στη Φορολογική Μνήμη της επέμβασης τεχνικού.

7.10.1. Το λογισμικό της ΕΑΦΔΣΣ ελέγχει, μέσω ειδικού αλγόριθμου, την πρόσβαση εξουσιοδοτημένων τεχνικών σ' αυτό. Ο κάτοχος της άδειας είναι υπεύθυνος για την παραχώρηση συγκεκριμένων συνδυασμών αλληλουχιών γραμμάτων και αριθμών (κωδικών πρόσβασης) στους εξουσιοδοτημένους απ' αυτόν τεχνικούς. Στις περιπτώσεις που απαιτούνται ειδικοί χειρισμοί προγραμματισμού για την επαναφορά σε κανονική λειτουργία της ΕΑΦΔΣΣ, έπειτα από βλάβη της μνήμης εργασίας (CMOS Error) ή σε περίπτωση ρυθμίσεων της ημερομηνίας και ώρας, ο εξουσιοδοτημένος τεχνικός εισάγει τον απαραίτητο κωδικό πρόσβασης. Μόνον στην περίπτωση που το λογισμικό της ΕΑΦΔΣΣ αναγνωρίσει τον συγκεκριμένο κωδικό, επιτρέπεται η

συνέχιση των λοιπών χειρισμών του εξουσιοδοτημένου τεχνικού, για την αποκατάσταση της βλάβης.

7.10.2. Το γεγονός αυτό αναγνωρίζεται από το λογισμικό της ΕΑΦΔΣΣ, ως «επέμβαση», αριθμείται και καταγράφεται στη φορολογική μνήμη. Υποχρεωτικά το λογισμικό της ΕΑΦΔΣΣ έχει δυνατότητα χειρισμού τουλάχιστον τριψήφιου αριθμού «επεμβάσεων» (μπορεί να αριθμήσει τουλάχιστον 1000 επεμβάσεις). Η αρίθμηση γίνεται υποχρεωτικά στο δεκαδικό αριθμητικό σύστημα και δεν επιτρέπεται αποτύπωση σε άλλο αριθμητικό σύστημα. Ο αύξων αθροιστικός προοδευτικός αριθμός επεμβάσεων αναγράφεται υποχρεωτικά σε κάθε «Z».

7.10.3. Η πλήρης και λεπτομερής περιγραφή του αλγορίθμου ελέγχου πρόσβασης εξουσιοδοτημένου τεχνικού, κατατίθεται στην Επιτροπή, στο φάκελο αίτησης χορήγησης άδειας καταλληλότητας.

8. Διαδικασία Ελέγχου Ακεραιότητας των εκδιδομένων στοιχείων με βάση τα αποθηκευμένα ηλεκτρονικά αρχεία.

8.1. Ο ελεγχόμενος παρέχει και θέτει σε άμεση χρήση κάθε μέσο και εξοπλισμό για τη διενέργεια του ελέγχου από τα αρμόδια ελεγκτικά όργανα.
Ο ελεγχόμενος υποχρεούται να :

- παραδίδει αντίγραφα των ηλεκτρονικών αρχείων των στοιχείων που του ζητούνται για έλεγχο σε κατάλληλο μέσο (πχ δισκέτες, οπτικούς δίσκους CD κλπ),
- βεβαιώνει και να αποδέχεται ότι είναι τα στοιχεία αυτά είναι ίδια με αυτά που εντοπίζονται και εκτυπώνονται στο βήμα iv.

8.2. Ο έλεγχος ενός στοιχείου μπορεί να περιλαμβάνει τα εξής :

i. Προσδιορισμός επί του ελεγχόμενου στοιχείου της ημερομηνίας έκδοσης του, καθώς και των στοιχείων της συμβολοσειράς Σήμανσης και της ΕΑΦΔΣΣ, από την οποία προέρχεται.

ii. Εκτύπωση Δελτίου Ανάγνωσης Περιόδου Φορολογικής Μνήμης Ημερήσιων Συνόψεων– (ΔΑΠΦΜΗΣ) για την ημερομηνία αυτή και προσδιορισμός επ' αυτού της Γενικής Ημερήσιας ΠΑΗΨΣ.

iii. Πρόσβαση στα φυλασσόμενα ηλεκτρονικά αρχεία στοιχείων και ΠΑΗΨΣ για την ημέρα αυτή και αφορούν την συγκεκριμένη ΕΑΦΔΣΣ

iv. Εντοπισμός και εκτύπωση των ηλεκτρονικών αρχείων κειμένου και ΠΑΗΨΣ του στοιχείου που ελέγχεται.

v. Ελέγχονται το περιεχόμενο του αρχείου κειμένου ("….._a.txt"), με το ελεγχόμενο στοιχείο. Ελέγχεται το περιεχόμενο, ανεξάρτητα από το μέγεθος και την εμφάνιση των χαρακτήρων. (Η συμβολοσειρά Σήμανσης δεν λαμβάνεται υπ' όψη). **Θα πρέπει να Ταυτίζονται !**

vi. Σύγκριση του περιεχομένου του ηλεκτρονικού αρχείου της ΠΑΗΨΣ ("….._b.txt"), με τη συμβολοσειρά Σήμανσης, η οποία αναγράφεται επί του ελεγχόμενου στοιχείου. **Θα πρέπει να Ταυτίζονται !**

vii. Χρήση Η/Υ για την εκτέλεση ειδικού προγράμματος δημιουργίας συνόψεων SHA-1, και δημιουργία γενικής ΠΑΗΨΣ από τις επιμέρους ΠΑΗΨΣ κάθε στοιχείου της ημέρας (στην οποία φυσικά συμμετέχει και η ΠΑΗΨΣ του ελεγχόμενου στοιχείου).

viii. Σύγκριση της προκύπτουσας ΠΑΗΨΣ του ελέγχου, με αυτήν που αναγράφεται στο Δελτίο Ανάγνωσης Περιόδου Φορολογικής Μνήμης Ημερήσιων Συνόψεων– (ΔΑΠΦΜΗΣ), του σημείου ii. **Θα πρέπει να Ταυτίζονται !**

9. Βιβλιάριο Συντήρησης και Επισκευών

9.1. Στο βιβλιάριο Συντήρησης και Επισκευών αναφέρονται με τρόπο επεξηγηματικό και κατανοητό όλοι οι απαραίτητοι χειρισμοί σε κατάσταση αποσύνδεσης από Η/Υ, για την έκδοση όλων των Ειδικών Φορολογικών Δελτίων, καθώς και για την ανάγνωση των Δεδομένων της Φορολογικής Μνήμης μέσω της σειριακής θύρας με χρήση Ηλεκτρονικού Υπολογιστή.

9.2. Επίσης σε ειδική σελίδα του βιβλιαρίου Συντήρησης και Επισκευών, αναγράφονται οι μέγιστες δυνατές τιμές που μπορούν να λάβουν οι εξής αθροιστές :

- Βλαβών CMOS
- Αποσυνδέσεων
- Αλλαγών Λεκτικών Επωνυμίας Κατόχου
- Καταγραφής προσβάσεων – επεμβάσεων Τεχνικού

9.3. Στο βιβλιάριο Συντήρησης και Επισκευών αναφέρονται υποχρεωτικά τα πλήρη στοιχεία και τα τηλέφωνα υποστήριξης του κατέχοντος την άδεια.

10. Έγκριση και χορήγηση άδειας καταλληλότητας

10.1. Διαδικασία

10.1.1. Η διαδικασία είναι η ίδια με αυτή που εφαρμόζεται μέχρι τώρα για τις ΦΤΜ, με βάση το ν. 1809/1988, μέσω της αίτησης και χορήγησης άδειας καταλληλότητας από την Ειδική Διακομματική Επιτροπή του άρθρου 7 του ίδιου νόμου.

10.2. Δικαιολογητικά

10.2.1 Για την Έγκριση και Χορήγηση Άδειας Καταλληλότητας, προσκομίζεται εκτός των λοιπών απαραίτητων δικαιολογητικών, πιστοποιητικών κλπ (σε Ειδικό Φάκελο Αίτησης Χορήγησης Άδειας Καταλληλότητας ΕΑΦΔΣΣ), υπεύθυνη δήλωση του ενδιαφερομένου, στην οποία βεβαιώνεται ότι η συγκεκριμένη ΕΑΦΔΣΣ, είναι απολύτως σύμφωνη με τις παρούσες τεχνικές προδιαγραφές.

10.3. Δείγμα Ελέγχου

10.3.1. Μαζί με τον Ειδικό Φάκελο Αίτησης προσκομίζεται και δείγμα της ΕΑΦΔΣΣ, το οποίο θα πρέπει να υποστεί τους εργαστηριακούς ελέγχους στο Εθνικό Μετσόβιο Πολυτεχνείο - Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, πρώτα για τα ηλεκτροπαροχικά (Εργαστήριο Υψηλών Τάσεων - Τομέας Ηλεκτρικής

Ισχύος) και μετά για τον έλεγχο ηλεκτρομαγνητικής συμβατότητας και λειτουργιών λογισμικού (Εργαστήριο Ασύρματης Επικοινωνίας - Τομέας Συστημάτων Μετάδοσης Πληροφορίας & Τεχνολογίας Υλικών).

10.4. Διάθεση Εξοπλισμού και Λογισμικού Ελέγχου

10.4.1 Για τους εργαστηριακούς ελέγχους στο ΕΜΠ, είναι απαραίτητη η διάθεση εξοπλισμού και δείγματος λογισμικού συνεργασίας και έκδοσης στοιχείων, σε προσωπικό ηλεκτρονικό υπολογιστή.

10.4.2. Για την τελική έγκριση επιδεικνύεται και ελέγχεται από την Επιτροπή και η συμπεριφορά και λειτουργία του δείγματος σε διασύνδεση με τον Η/Υ.

11. Παρακολούθηση ΕΑΦΔΣΣ μέσω του συστήματος TAXIS.

11.1. Για την παρακολούθηση των ΕΑΦΔΣΣ που εγκαθίστανται σε επιχειρήσεις και επιτηδευματίες, ακολουθείται ακριβώς η ίδια διαδικασία που εφαρμόζεται ήδη και στις Φορολογικές Ταμειακές Μηχανές μέσω του συστήματος TAXIS. Οι κάτοχοι ΕΑΦΔΣΣ υποχρεούνται εντός 10ημέρου να δηλώσουν την αγορά νέας ή μεταχειρισμένης ΕΑΦΔΣΣ, στην αρμόδια ΔΟΥ της περιοχής τους, καθώς και κάθε μεταβολή – αλλαγή κατόχου ή έδρας λειτουργίας της ΕΑΦΔΣΣ.

ΠΑΡΑΡΤΗΜΑ Π1
Ασφαλής Hash Αλγόριθμος SHA-1

Π1. Εισαγωγική Περιγραφή

Το παρόν κείμενο βασίζεται στο έγγραφο – πρότυπο **FIPS-180-2** (Federal Information Processing Standards) που εκδόθηκε από το National Institute of Standards and Technology (NIST) μετά την υιοθέτησή του από το Υπουργείο των ΗΠΑ (Secretary of Commerce) σύμφωνα με την παράγραφο 5131 του Information Technology Management Reform Act of 1996 (Public Law 104-106), και του Computer Security Act of 1987 (Public Law 100-235), και περιορίζεται στην **εισαγωγική περιγραφή μόνον του Ασφαλούς hash Αλγορίθμου SHA-1**, από τους τέσσερις – 4 συνολικά ασφαλείς αλγόριθμους (SHA-1, SHA-256, SHA-384, και SHA-512) που προδιαγράφονται στο πρότυπο αυτό.

Π1.1. Γενικά για τους Ασφαλείς Αλγόριθμους SHA

Όλοι οι παραπάνω αλγόριθμοι είναι επαναληπτικές hash συναρτήσεις ενός δρόμου (μονόδρομες συναρτήσεις), οι οποίες μπορούν να επεξεργαστούν ένα μήνυμα και να δώσουν μια συμπυκνωμένη αναπαράσταση – έκφραση, η οποία καλείται **σύνοψη μηνύματος** (message digest) και προσδιορίζει **μονοσήμαντα** το μήνυμα από το οποίο προήλθε (υπογραφή του μηνύματος). Αυτοί οι αλγόριθμοι επιτρέπουν τον απόλυτο καθορισμό της ακεραιότητας του μηνύματος : κάθε αλλαγή στο (αρχικό) μήνυμα θα επιφέρει σαν αποτέλεσμα – με πάρα πολύ μεγάλη πιθανότητα – μια διαφορετική σύνοψη (διαφορετική υπογραφή). Αυτή η ιδιότητα είναι πολύ χρήσιμη για την δημιουργία και τον έλεγχο ψηφιακών υπογραφών και κωδικών πιστοποίησης μηνυμάτων, καθώς και στην δημιουργία τυχαίων αριθμών (bits).

Κάθε αλγόριθμος μπορεί να περιγραφεί γενικά σε δύο βήματα -στάδια : την προ-επεξεργασία και τον υπολογισμό της τιμής hash. Η προ-επεξεργασία περιλαμβάνει τη συμπλήρωση («γέμισμα») του μηνύματος, το τεμάχισμα, την ανάλυση του «γεμισμένου» μηνύματος σε τμήματα (blocks) των m – bit, και τον καθορισμό – την απόδοση αρχικών τιμών που θα χρησιμοποιηθούν στον υπολογισμό της τιμής hash. Ο υπολογισμός της hash τιμής, δημιουργεί ένα διάγραμμα του μηνύματος από το «γεμισμένο» μήνυμα και χρησιμοποιεί αυτό το διάγραμμα, σε συμφωνία με τις συναρτήσεις, τις σταθερές και τους χειρισμούς λέξεων για την επαναληπτική δημιουργία σειρών από τιμές hash. Η τελική hash τιμή που δημιουργείται, αποτελεί τον υπολογισμό hash που χρησιμεύει για τον καθορισμό της σύνοψης (υπογραφής) του μηνύματος.

Η σημαντικότερη διαφορά μεταξύ των τεσσάρων - 4 αλγορίθμων, έγκειται στον αριθμό των bit ασφαλείας που παρέχονται για τα δεδομένα που θα υποστούν την διαδικασία hash – αυτό σχετίζεται κατευθείαν με το μήκος της σύνοψης (υπογραφής) του μηνύματος. Όταν ένας ασφαλής hash αλγόριθμος χρησιμοποιείται σε συσχέτιση με έναν άλλο αλγόριθμο, μπορεί να υπάρχουν απαιτήσεις, καθοριζόμενες αλλού, οι οποίες να απαιτούν τη χρήση ενός ασφαλούς hash αλγόριθμου, με συγκεκριμένο αριθμό bit ασφαλείας. Για παράδειγμα, εάν ένα μήνυμα πρόκειται να «υπογραφεί» μ' έναν αλγόριθμο ψηφιακής υπογραφής, ο οποίος παρέχει 128 bit ασφάλεια, τότε αυτός ο αλγόριθμος ψηφιακής υπογραφής, απαιτεί την χρήση ενός ασφαλούς hash αλγορίθμου, ο οποίος επίσης παρέχει και ανταποκρίνεται στην 128 bit ασφάλεια (πχ SHA-256).

Επιπρόσθετα, οι τέσσερις αυτοί αλγόριθμοι διαφέρουν στο μέγεθος των τμημάτων (blocks) και λέξεων των δεδομένων, που χρησιμοποιούνται κατά την διάρκεια της διαδικασίας hash. Το Σχήμα 1 παρουσιάζει τις βασικές ιδιότητες όλων αυτών των 4 αλγορίθμων.

Αλγόριθμος	Μέγεθος Μηνύματος (bits)	Μέγεθος Τμήματος – block (bits)	Μέγεθος Λέξης (bits)	Μέγεθος Σύνοψης Μηνύματος (bits)	Ασφάλεια (bits)
SHA-1	**$< 2^{64}$**	**512**	**32**	**160**	**80**
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

Σχήμα 1 : Ιδιότητες των Ασφαλών Hash Αλγορίθμων.

Π1.2. Ορισμοί

Π1.2.1 Λεξιλόγιο των χρησιμοποιούμενων όρων και ακρωνυμίων

Bit — Ένα δυαδικό ψηφίο που παίρνει τιμές είτε 0 είτε 1.

Byte — Ένα σύνολο – μια ομάδα από οκτώ bit.

Word — Ένα σύνολο – μια ομάδα από 32 bit (4 byte) (είτε από 64 bit - 8 byte), το οποίο εξαρτάται από τον ασφαλή hash αλγόριθμο που χρησιμοποιείται. *Στον SHA-1 1 word = 32 bit (= 4 byte).*

Π1.2.2 Αλγοριθμικές Παράμετροι, Χρησιμοποιούμενα Σύμβολα, και Όροι

Π1.2.2.1 Παράμετροι

Οι επόμενοι παράμετροι χρησιμοποιούνται στην λεπτομερή παρουσίαση του ασφαλούς hash αλγορίθμου αυτού του προτύπου :

a, b, c, ..., h — Μεταβλητές εργασίας (συνολικά μέχρι οκτώ – 8), οι οποίες είναι λέξεις των w-bit που χρησιμοποιούνται στον υπολογισμό των τιμών hash, H(i). *Για τον SHA-1 χρησιμοποιούνται μόνον οι πέντε – 5 μεταβλητές εργασίας : a, b, c,d και e.*

$H^{(i)}$ — Η i-οστή hash τιμή. Η τιμή $H_{(0)}$ είναι η αρχική hash τιμή. Η τιμή $H_{(N)}$ είναι η τελική hash τιμή και χρησιμοποιείται για τον καθορισμό της σύνοψης του μηνύματος. *Στον SHA-1, το κάθε μήνυμα αφού «γεμιστεί» για να καταστεί πολλαπλάσιο του αριθμού 512, τεμαχίζεται σε N τμήματα των 512 bits το καθένα.*

$H^{(i)}{}_j$ — Η j-οστή λέξη της i-οστής hash τιμής, όπου $H^{(i)}{}_0$ είναι η πλέον αριστερή (η αριστερότερη) λέξη της i-οστής hash τιμής.

K_t — Σταθερή τιμή που χρησιμοποιείται στην t-οστή επανάληψη του υπολογισμού hash.

k	Ο αριθμός των μηδενικών – 0, που θα προστεθούν – συμπληρωθούν στο μήνυμα, κατά την διάρκεια του βήματος του «γεμίσματος».
l	Το μήκος – μέγεθος του μηνύματος, M, σε bit.
m	Ο αριθμός των bits σ' ένα τμήμα (block), $M_{(i)}$ ου μηνύματος. *Στον SHA-1, ο αριθμός αυτός είναι m = 512.*
M	Το μήνυμα που πρόκειται να υποστεί την διαδικασία hash.
$M^{(i)}$	Το τμήμα (block), i, του μηνύματος που έχει μέγεθος m bit.
$M^{(i)}{}_j$	Η j-οστή λέξη του i-οστού τμήματος (block) i, του μηνύματος όπου $M^{(i)}{}_0$ είναι η πλέον αριστερή (η αριστερότερη) λέξη του i-οστού τμήματος (block) i.
n	Ο αριθμός των bit που θα περιστραφούν (rotation) ή θα ολισθήσουν (shift) σε μια λέξη, όταν αυτή θα υποστεί την διαδικασία της περιστροφής ή της ολίσθησης.
N	Ο αριθμός των τμημάτων (block), σ' ένα «γεμισμένο» μήνυμα.
T	Προσωρινή λέξη των w-bit που χρησιμοποιείται στους hash υπολογισμούς.
w	Ο αριθμός των bit σε μια λέξη. *Στον SHA-1, ο αριθμός αυτός είναι w = 32.*
W_t	Η t-οστή λέξη των w-bit του διαγράμματος του μηνύματος.

Π1.2.2.2 Σύμβολα πράξεων

Τα ακόλουθα σύμβολα χρησιμοποιούνται στην λεπτομερή παρουσίαση του ασφαλούς hash αλγορίθμου, και καθένα ενεργεί στις λέξεις των w-bit.

$\wedge$	Η Δυαδική – Λογική πράξη «ΚΑΙ» (AND).
$\vee$	Η Δυαδική – Λογική πράξη «Ή» (OR).
$\oplus$	Η Δυαδική – Λογική πράξη «Αποκλειστικό Ή» (XOR).
$\neg$	Η Δυαδική – Λογική πράξη της Συμπλήρωσης.
+	Η Δυαδική Αριθμητική πράξη πρόσθεσης «modulo 2^w. *(Σημ. Περισσότερα στην παράγραφο 7.2.).*
<<	Η Δυαδική πράξη Αριστερής Ολίσθησης (Left-shift), όπου στην πράξη $x << n$ πρώτα αποβάλλονται τα n αριστερότερα bit από τη λέξη x και μετά το αποτέλεσμα λαμβάνεται προσθέτοντας («γεμίζοντας») με n αριθμό μηδενικών στα δεξιά.

>> Η Δυαδική πράξη Δεξιάς Ολίσθησης (Right-shift), όπου στην πράξη $x >> n$ πρώτα αποβάλλονται τα n δεξιότερα bit από τη λέξη x και μετά το αποτέλεσμα λαμβάνεται προσθέτοντας («γεμίζοντας») με n αριθμό μηδενικών στα αριστερά.

Π1.3. Συμβολισμοί και Κανόνες Παράστασης

Π1.3.1 Αλληλουχίες (σειρές) από Bit και Ακέραιοι.

Η ακόλουθη ορολογία που χρησιμοποιείται συσχετίζεται με Αλληλουχίες (σειρές) από Bit και Ακέραιους

1. Δεκα-εξαδικό ψηφίο (*hex digit*) είναι ένα στοιχείο – σύμβολο από το σύνολο :{`0, 1,…, 9, a,…, f`}. Επίσης ένα δεκα-εξαδικό ψηφίο θεωρείται και αναπαράσταση μιας αλληλουχίας (σειράς) τεσσάρων – 4 bit. Για παράδειγμα, το δεκα-εξαδικό ψηφίο "`7`" αναπαριστά την 4-bit αλληλουχία "`0111`", και το δεκα-εξαδικό ψηφίο "`a`" αναπαριστά την 4-bit αλληλουχία "`1010`".

2. Λέξη (*word*) είναι μία *w*-bit αλληλουχία, η οποία μπορεί να αναπαρασταθεί σαν μια σειρά από δεκαεξαδικά ψηφία. Για την μετατροπή μιας λέξης σε δεκαεξαδικά ψηφία, κάθε «κομματάκι» των 4-bit, μετατρέπεται στο αντίστοιχο (ισοδύναμο) με αυτό, δεκαεξαδικό ψηφίο, όπως αναφέρθηκε παραπάνω στην προηγούμενη (1)παράγραφο. Για παράδειγμα η 32-bit λέξη :

```
1010 0001 0000 0011 1111 1110 0010 0011
```

μπορεί να παρασταθεί σαν "`a103fe23`", και η 64-bit λέξη

```
1010 0001 0000 0011 1111 1110 0010 0011
0011 0010 1110 1111 0011 0000 0001 1010
```

μπορεί να παρασταθεί σαν "`a103fe2332ef301a`".

(Σημ. Παντού μέσα σ' αυτή τη λεπτομερή παρουσίαση χρησιμοποιείται η σύμβαση της παράστασης των δυαδικών λέξεων 32- και 64- bit, έτσι ώστε το πλέον σημαντικό bit είναι αυτό που ευρίσκεται στην πλέον αριστερή – αριστερότερη θέση της αλληλουχίας).

3. Ένας Ακέραιος (*integer*) μπορεί να παρασταθεί σαν μία λέξη ή σαν ζευγάρι από λέξεις. Μία λέξη αναπαράστασης του μήκους l του μηνύματος, σε bits, απαιτείται στις τεχνικές συμπλήρωσης («γεμίσματος») του Κεφάλαιο 5.1.
Ένας ακέραιος μεταξύ του 0 και του 2^{32}-1 (*συμπεριλαμβανομένου*), μπορεί να αναπαρασταθεί σαν μια 32-bit λέξη. Η λιγότερο σημαντική τετράδα bit του ακεραίου αναπαριστάται με το πλέον δεξιό (δεξιότερο) δεκαεξαδικό ψηφίο της λέξης αναπαράστασης. Για παράδειγμα, ο ακέραιος $291 = 2^8 + 2^5 + 2^1 + 2^0 = 256+32+2+1$ αναπαριστάται με την δεκαεξαδική λέξη : `00000123.`
Το ίδιο ισχύει για έναν ακέραιο μεταξύ του 0 και του 2^{64}-1 (*συμπεριλαμβανομένου*), ο οποίος μπορεί να αναπαρασταθεί σαν μια 64-bit λέξη.
Εάν Z είναι ένας ακέραιος, $0 \le Z < 2^{64}$, τότε $Z = 2^{32}X + Y$ όπου $0 \le X < 2^{32}$ and $0 \le Y < 2^{32}$.

Επειδή X και Y μπορούν να αναπαρασταθούν σαν 32-bit λέξεις, x και y αντίστοιχα, ο ακέραιος Z μπορεί να αναπαρασταθεί σαν ζευγάρι λέξεων αριθμών (x, y). Αυτή ακριβώς η ιδιότητα χρησιμοποιείται στον αλγόριθμο SHA-1 (και SHA-256).

4. Για τους ασφαλείς hash αλγορίθμους, το μέγεθος του τμήματος (block) του μηνύματος των m-bits, εξαρτάται από τον ίδιο τον αλγόριθμο.
Για τον αλγόριθμο SHA-1 (και SHA-256), κάθε τμήμα (block) του μηνύματος έχει μέγεθος m = 512 bits, το οποίο και μπορεί να αναπαρασταθεί από μια ακολουθία από δεκαέξι - 16 λέξεις των 32-bits. (16 x 32 = 512)
(Για τους αλγόριθμους SHA-384 και SHA-512, κάθε τμήμα (block) του μηνύματος έχει μέγεθος m = 1024 bits, το οποίο και μπορεί να αναπαρασταθεί από μια ακολουθία από δεκαέξι - 16 λέξεις των 64-bits).

Π1.3.2 Πράξεις επί των Λέξεων.

Οι ακόλουθες πράξεις εφαρμόζονται επί των w-bit λέξεων σε όλους και στους τέσσερις – 4 hash αλγόριθμους. Οι SHA-1 και SHA-256 λειτουργούν σε 32-bit λέξεις (w = 32 bit), και οι SHA-384 και SHA-512 λειτουργούν σε 64-bit λέξεις (w = 64 bit) :

1. Οι Δυαδικές – Λογικές πράξεις : $\wedge$, $\vee$, $\oplus$, and $\neg$ (δες παράγρ. Π1.2.2).

2. Η Δυαδική Αριθμητική πράξη (+) πρόσθεσης «modulo 2^w». Η πράξη $x + y$ ορίζεται ως ακολούθως : οι λέξεις x και y, αναπαριστούν τους ακεραίους X και Y, όπου $0 \le X < 2^w$ and $0 \le Y < 2^w$. Για δύο θετικούς ακεραίους U και V, ορίστε την πράξη U mod V να αντιστοιχεί στο υπόλοιπο της διαίρεσης του U διά του V και υπολογίστε

   $$Z = (X + Y) \bmod 2^w$$

   όπου $0 \le Z < 2^w$. Μετατρέψτε τον ακέραιο Z σε λέξη, z, και ορίστε την πράξη $z = x + y$.

3. Η πράξη της Δεξιάς Ολίσθησης $\boldsymbol{SHR^n(x)}$, (όπου x είναι μια λέξη και n είναι ένας ακέραιος $0 \le n < w$), ορίζεται ως :

   $$SHR^n(x) = x >> n.$$

   Η πράξη αυτή χρησιμοποιείται στους αλγορίθμους SHA-256, SHA-384, και SHA-512.

4. Η πράξη της Δεξιάς Κύλισης $\boldsymbol{ROTR^n(x)}$, (όπου x είναι μια λέξη και n είναι ένας ακέραιος $0 \le n < w$), ορίζεται ως :

   $$ROTR^n(x) = x >> n \vee (x << w - n).$$

   Η πράξη αυτή είναι ισοδύναμη με μια κυκλική ολίσθηση (Κύλιση) του x με n θέσεις προς τα δεξιά. Η πράξη αυτή χρησιμοποιείται στους αλγορίθμους SHA-256, SHA-384, και SHA-512.

5. Η πράξη της Αριστερής Κύλισης $\boldsymbol{ROTL^n(x)}$, (όπου x είναι μια λέξη και n είναι ένας ακέραιος $0 \le n < w$), ορίζεται ως :

$$ROTL^{n}(x) = x << n \vee (x >> w - n).$$

Η πράξη αυτή είναι ισοδύναμη με μια κυκλική ολίσθηση (Κύλιση) του x με n θέσεις προς τ' αριστερά. *Η πράξη αυτή χρησιμοποιείται μόνον στον αλγόριθμο SHA-1.*

6. Σημειώνεται η ακόλουθη ισοδυναμία (≈) των σχέσεων, όπου w είναι καθορισμένο σε κάθε σχέση :

$$ROTL^{n}(x) \approx ROTR^{w-n}(x).$$
$$ROTR^{n}(x) \approx ROTL^{w-n}(x).$$

Π1.4. Συναρτήσεις και Σταθερές

Π1.4.1 Συναρτήσεις που χρησιμοποιούνται στον αλγόριθμο SHA-1.

Ο αλγόριθμος SHA-1 χρησιμοποιεί μια σειρά από λογικές συναρτήσεις $f_0, f_1, \ldots, f_{79}$. Κάθε συνάρτηση f_t όπου $0 \le t < 79$, επενεργεί σε τρεις – 3 λέξεις των 32-bit , x, y, και z, και παράγει μια μόνο λέξη των 32-bit σαν έξοδο. Η συνάρτηση $f_t(x, y, z)$ ορίζεται ως ακολούθως :

$$f_t(x,y,z) = \begin{cases} (x \wedge y) \vee (\neg x \wedge z) & 0 \le t \le 19 \\ x \oplus y \oplus z & 20 \le t \le 39 \\ (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) & 40 \le t \le 59 \\ x \oplus y \oplus z & 60 \le t \le 79. \end{cases}$$

Π1.4.2 Σταθερές που χρησιμοποιούνται στον αλγόριθμο SHA-1.

Ο αλγόριθμος SHA-1 χρησιμοποιεί ογδόντα – 80 σταθερές – λέξεις των 32-bit, K_0, $K_1, \ldots, K_{79}$ οι οποίες καθορίζονται ως ακολούθως :

$$K_t = \begin{cases} \texttt{5a827999} & 0 \le t \le 19 \\ \texttt{6ed9eba1} & 20 \le t \le 39 \\ \texttt{8f1bbcdc} & 40 \le t \le 59 \\ \texttt{ca62c1d6} & 60 \le t \le 79. \end{cases}$$

Π1.5. Προεπεξεργασία

Η προεπεξεργασία πρέπει να λαμβάνει χώρα πριν ξεκινήσει ο υπολογισμός της hash τιμής. Η προεπεξεργασία συνίσταται από τρία – 3 βήματα : α) Το «γέμισμα» του μηνύματος *M* (δες 5.1), β) Την ανάλυση (το «τεμάχισμα») του μηνύματος σε τμήματα (blocks) (δες 5.2)και γ) την απόδοση αρχικών hash τιμών $H^{(0)}$ (δες 5.3).

Π1.5.1 Συμπληρώνοντας το μήνυμα («γέμισμα» του μηνύματος).

Το μήνυμα, *M*, θα πρέπει να «γεμιστεί» στο τέλος του, με μηδενικά, προτού αρχίσουν οι υπολογισμοί. Ο σκοπός αυτού του «γεμίσματος» είναι για να καταστεί βέβαιο ότι το

«γεμισμένο» μήνυμα θα πρέπει να αποτελεί πολλαπλάσιο του αριθμού των 512 ή 1024 bits, ανάλογα με τον χρησιμοποιούμενο αλγόριθμο.

Π1.5.1.1 SHA-1 (και SHA-256)

Υποθέστε, ότι το μήκος του μηνύματος, M, είναι ℓ bits. Προσθέτουμε το bit "1", ακολουθούμενο από k-bit μηδενικά, όπου k είναι το μικρότερο, μη αρνητικό αποτέλεσμα της εξίσωσης $l + 1 + k \equiv 448 \bmod 512$. Μετά προσθέτουμε το μήκους 64-bit τμήμα (block), το οποίο είναι ίσο με τον αριθμό l, εκπεφρασμένο σε 64-μπιτη δυαδική παράσταση.
Για παράδειγμα το (8-bit ASCII) μήνυμα "**abc**" έχει μήκος 8 x 3 = 24 bits, επομένως το μήνυμα γεμίζεται πρώτα με το bit "1" και μετά με 448 – (24+1) = 423 μηδενικά bits. Μετά με τον αριθμό του μήκους του μηνύματος (24), εκπεφρασμένο όπως είπαμε, σε 64-μπιτη δυαδική παράσταση, για να διαμορφωθεί τελικά ένα 512-bit μήκους, μήνυμα.

				423	64
01100001	01100010	01100011	1	00…00	00…011000
"a"	"b"	"c"			l = 24

(Το μήκος του «γεμισμένου» μηνύματος θα πρέπει να είναι πολλαπλάσιο του αριθμού των 512-bit).

Π1.5.2 Ανάλυση (τμηματοποίηση) του «γεμισμένου» μηνύματος

Μετά το «γέμισμα», το μήνυμα πρέπει να «σπάσει» σε N τμήματα - κομμάτια (blocks) των m-bit το καθένα, πριν αρχίσουν οι υπολογισμοί hash.

Π1.5.2.1 SHA-1 (και SHA-256)

Για τους αλγόριθμους SHA-1 και SHA-256, το «γεμισμένο» μήνυμα τεμαχίζεται σε N τμήματα (blocks) των 512-bit , $M^{(1)}$, $M^{(2)}$,…, $M^{(i)}$, …, $M^{(N)}$. Επειδή ένα τμήμα (block) 512-bit μπορεί να εκφρασθεί με 16 λέξεις των 32-bit η κάθε μια, (16 x 32 = 512), τα πρώτα 32 bits του block i, μπορούν να συμβολιστούν με $M^{(i)}_{(0)}$, τα επόμενα 32 bits $M^{(i)}_{(1)}$, και ούτω καθ' εξής, μέχρι το $M^{(i)}_{(15)}$.

Π1.5.3 Ορισμός και απόδοση Αρχικής Hash Τιμής $(H^{(0)})$

Πριν ξεκινήσουν οι υπολογισμοί hash, για καθέναν από τους ασφαλείς αλγόριθμους, πρέπει να ορισθεί η αρχική τιμή hash $(H^{(0)})$. Το μέγεθος και ο αριθμός των λέξεων στην αρχική hash τιμή $H^{(0)}$, εξαρτάται από το μέγεθος της σύνοψης (υπογραφής) του μηνύματος.

Π1.5.3.1 SHA-1

Για τον αλγόριθμο SHA-1, η αρχική hash τιμή $H^{(0)}$, αποτελείται από 5 δεκαεξαδικές λέξεις των 32-bit :

$$H^{(0)}_0 = \texttt{67452301}$$
$$H^{(0)}_1 = \texttt{efcdab89}$$
$$H^{(0)}_2 = \texttt{98badcfe}$$
$$H^{(0)}_3 = \texttt{10325476}$$
$$H^{(0)}_4 = \texttt{c3d2e1f0}$$

Π1.6. Ασφαλείς HASH Αλγόριθμοι.

Για καθέναν από τους ασφαλείς αλγόριθμους, υπάρχει δυνατότητα εναλλακτικών μεθόδων υπολογισμών, οι οποίες όμως δίνουν το ίδιο ακριβώς αποτέλεσμα. Ένα παράδειγμα μιας εναλλακτικής SHA-1 μεθόδου υπολογισμού περιγράφεται στην παράγραφο. Π1.6.1.3. Τέτοιες μέθοδοι υπολογισμών, μπορούν να υλοποιούνται σε συμμόρφωση με την παρούσα προδιαγραφή.

Π1.6.1 SHA-1

Ο SHA-1 μπορεί να χρησιμοποιηθεί σ' ένα μήνυμα M, το οποίο έχει μήκος l-bits, όπου $0 \le l \ge 2^{64}$. *(Σημ. 2^{64} = 18.446.744.073.709.551.616 bits ή 2.305.843.009.213.693.952 bytes)*.

Ο αλγόριθμος χρησιμοποιεί 1) ένα πίνακα-διάγραμμα από 80 λέξεις των 32-bit η κάθε μια, 2) 5 μεταβλητές εργασίας των 32-bit η κάθε μια, και 3) 1 hash τιμή επίσης των 32-bit η κάθε μια. Το τελικό αποτέλεσμα του SHA-1 είναι μια σύνοψη (υπογραφή) των 160-bit.

Οι 80 λέξεις του πίνακα-διαγράμματος, συμβολίζονται με W_0, W_1,…, W_{79}. Οι 5 λέξεις των μεταβλητών εργασίας συμβολίζονται με ***a***, ***b***, ***c***, ***d***, και ***e***. Οι λέξεις της τιμής hash συμβολίζονται με $H^{(i)}{}_0$, $H^{(i)}{}_1$, $H^{(i)}{}_2$, $H^{(i)}{}_3$, $H^{(i)}{}_4$. Οι λέξεις της τιμής hash ξεκινούν έχοντας την αρχική hash τιμή : $H^{(0)}{}_0$, $H^{(0)}{}_1$, $H^{(0)}{}_2$, $H^{(0)}{}_3$, $H^{(0)}{}_4$, αντικαθιστώνται με κάθε επόμενη – ενδιάμεση τιμή hash, για κάθε τμήμα (block) που επεισέρχεται στην επεξεργασία υπολογισμών hash και τελειώνουν με την τελική hash τιμή $H^{(N)}$. Ο SHA-1 επίσης ακόμη, χρησιμοποιεί μια απλή προσωρινή λέξη που συμβολίζεται με T.

Το **Παράρτημα Α**, αυτού του κειμένου δίνει λεπτομερή παραδείγματα του αλγόριθμου SHA-1.

Π1.6.1.1 SHA-1 Προ-επεξεργασία

1. «Γέμισμα» του μηνύματος M, σύμφωνα με την παράγραφο Π1.5.1.1.
2. Τεμάχισμα του «γεμισμένου» μηνύματος σε N τμήματα των 512-bit : $M^{(1)}$, $M^{(2)}$,…, $M^{(N)}$, σύμφωνα με την παράγραφο Π1.5.2.1. και
3. Ορισμός της αρχικής hash τιμής $H^{(0)}$, όπως προδιαγράφτηκαν στην παράγραφο Π1.5.3.1.

Π1.6.1.2 SHA-1 Υπολογισμός Hash

Ο υπολογισμός του αλγόριθμου SHA-1 χρησιμοποιεί συναρτήσεις και σταθερές που προσδιορίστηκαν προηγουμένως στην παράγραφο Π1.4.1.1 και Π1.4.2.1, αντίστοιχα. Η πρόσθεση γίνεται με βάση τους κανόνες της Αριθμητικής «modulo 2^{32}».
Μετά το τέλος του σταδίου της προ-επεξεργασίας, κάθε τμήμα (block) $M^{(1)}$, $M^{(2)}$,…, $M^{(N)}$, επεξεργάζεται, το καθένα με τη σειρά του, κάνοντας τα εξής βήματα :

For i = 1 to N:

{

1. Προετοιμασία του πίνακα – διαγράμματος, $\{W_t\}$:

$$W_t = \begin{cases} M^{(i)}{}_{(t)}. & 0 \le t \le 15 \\ ROTL^1 (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) & 16 \le t \le 79 \end{cases}$$

2. Ορισμός αρχικών τιμών στις 5 μεταβλητές εργασίας, ***a***, ***b***, ***c***, ***d***, and ***e***, για κάθε (i-1)-στή hash τιμή :

   $a = H^{(i)}_0$
   $b = H^{(i)}_1$
   $c = H^{(i)}_2$
   $d = H^{(i)}_3$
   $e = H^{(i)}_4$

3. For t = 0 to 79:
   {
   $T = ROTL^5\ (a) + f_t(b,c,d) + e + K_t + W_t$
   $e = d$
   $d = c$
   $c = ROTL^{30}(b)$
   $b = a$
   $a = T$
   }

4. Υπολογισμός της *i-στής* ενδιάμεσης hash τιμής $H^{(i)}$:

   $H^{(i)}_0 = a + H^{(i-1)}_0$
   $H^{(i)}_1 = b + H^{(i-1)}_1$
   $H^{(i)}_2 = c + H^{(i-1)}_2$
   $H^{(i)}_3 = d + H^{(i-1)}_3$
   $H^{(i)}_4 = e + H^{(i-1)}_4$

}

Μετά την ολοκλήρωση όλων των επαναλήψεων των βημάτων 1 έως 4, για N φορές συνολικά, (δηλ. μετά την ολοκλήρωση της επεξεργασίας το μηνύματος $M^{(N)}$), το αποτέλεσμα της σύνοψης (υπογραφής) των 160-bit, ολόκληρου του μηνύματος M, είναι η συνένωση των τελικών hash τιμών :

$$H^{(N)}_0 \parallel H^{(N)}_1 \parallel H^{(N)}_2 \parallel H^{(N)}_3 \parallel H^{(N)}_4$$

Π1.6.1.3 Εναλλακτική μέθοδος υπολογισμού του αλγορίθμου SHA-1 για τη σύνοψη (υπογραφή) ενός μηνύματος.

Η μέθοδος υπολογισμού για τον αλγόριθμο SHA-1, που περιγράφτηκε προηγουμένως στην παράγραφο Π1.6.1.2, προϋποθέτει ότι ο πίνακας – διάγραμμα για το μήνυμα, (W_0, W_1,…, W_{79}), υλοποιείται από έναν πίνακα 80 λέξεων των 32-bit. Αυτό είναι αποτελεσματικό από την σκοπιά της ελαχιστοποίησης του χρόνου εκτέλεσης του αλγορίθμου, αφού οι τιμές $W_{t-3}, W_{t-8}, W_{t-14}, W_{t-16}$, στο βήμα (2) της παραγράφου Π1.6.1.2, είναι εύκολα υπολογίσιμες.

Ωστόσο, εάν η διαθέσιμη μνήμη είναι περιορισμένη, τότε μια εναλλακτική προσέγγιση μπορεί να υλοποιηθεί, θεωρώντας τον πίνακα – διάγραμμα $\{Wt\}$ σαν ένα πίνακα που αποτελείται από 16 λέξεις των 32-bit η κάθε μια : W_0, W_1,…, W_{15}. Η εναλλακτική

μέθοδος που περιγράφεται σ' αυτή την παράγραφο, δίνει ακριβώς την ίδια σύνοψη (υπογραφή) του SHA-1, όπως αυτή περιγράφτηκε στην προηγούμενη παράγραφο Π1.6.1.2. Αν και αυτή η εναλλακτική μέθοδος μας γλιτώνει αποθηκευτικό χώρο 64 λέξεων των 32-bit η κάθε μια, πιθανότατα επιμηκύνει τον χρόνο εκτέλεσης, εξαιτίας της αυξημένης πολυπλοκότητας των υπολογισμών για τον πίνακα – διάγραμμα *{Wt}* στο βήμα (3).

Γι αυτή την εναλλακτική μέθοδο υπολογισμού SHA-1, θέτουμε *MASK = 0000000f* (δεκαεξαδική τιμή). Όπως και στην παράγραφο Π1.6.1.1, η πρόσθεση γίνεται με βάση τους κανόνες της Αριθμητικής «modulo 2^{32}». Υποθέτοντας ότι η προεπεξεργασία που περιγράφτηκε στην παράγραφο Π1.6.1.1, έχει ήδη επιτελεστεί, η επεξεργασία του $M^{(i)}$ γίνεται ως ακολούθως :

For i = 1 to N:
{

1. For t = 0 to 15 :
   {
   $W_t = M^{(i)}_{(t)}$.
   }

2. Ορισμός αρχικών τιμών στις 5 μεταβλητές εργασίας, ***a***, ***b***, ***c***, ***d***, and ***e***, για κάθε (i-1)-στή hash τιμή :

   $a = H^{(i)}_0$
   $b = H^{(i)}_1$
   $c = H^{(i)}_2$
   $d = H^{(i)}_3$
   $e = H^{(i)}_4$

3. For t = 0 to 79:
   {
   $s = t \wedge MASK$

   if $t \geq 16$ *then*
   {
   $W_s = ROTL^1(W_{(s+13)\wedge MASK} \oplus W_{(s+8)\wedge MASK} \oplus W_{(s+2)\wedge MASK} \oplus W_{(s)})$
   }

   $T = ROTL^5(a) + f_t(b,c,d) + e + K_t + W_s$
   $e = d$
   $d = c$
   $c = ROTL^{30}(b)$
   $b = a$
   $a = T$
   }

4. Υπολογισμός της *i-στής* ενδιάμεσης hash τιμής $H^{(i)}$:

   $H^{(i)}_0 = a + H^{(i-1)}_0$
   $H^{(i)}_1 = b + H^{(i-1)}_1$

$H^{(i)}_2 = c + H^{(i-1)}_2$
$H^{(i)}_3 = d + H^{(i-1)}_3$
$H^{(i)}_4 = e + H^{(i-1)}_4$

}

Μετά την ολοκλήρωση όλων των επαναλήψεων των βημάτων 1 έως 4, για N φορές συνολικά, (δηλ. μετά την ολοκλήρωση της επεξεργασίας το μηνύματος $M^{(N)}$), το αποτέλεσμα της σύνοψης (υπογραφής) των 160-bit, ολόκληρου του μηνύματος M, είναι η συνένωση των τελικών hash τιμών :

$$H^{(N)}_0 \parallel H^{(N)}_1 \parallel H^{(N)}_2 \parallel H^{(N)}_3 \parallel H^{(N)}_4$$

Π1.Α. Παράρτημα Α : Παραδείγματα SHA-1.

Αυτό το παράρτημα είναι μόνον για ενημερωτικούς σκοπούς και δεν απαιτείται να συμφωνεί με το παρόν πρότυπο.

Π1.Α.1 SHA-1 Παράδειγμα Μηνύματος ενός μόνον τμήματος (1-block message)

Έστω ότι το μήνυμα M, είναι η 24-bit (μέγεθος – μήκος l =24) ASCII συμβολοσειρά «**abc**», το οποίο είναι ισοδύναμο με την ακόλουθη δυαδική παράσταση :

`01100001 01100010 01100011`.

Το μήνυμα γεμίζεται πρώτα προσθέτοντας το bit “1”, μετά με 448 – (24+1) = 423 μηδενικά bits – “0”, και τέλος με την δεκαεξαδική τιμή $(00000000\ 00000018)_{hex}$ που αντιστοιχεί στις 2 λέξεις των 32-bit του αριθμού (δεκαδικού) 24 που είναι το αρχικό μέγεθος του αρχικού μηνύματος. Έτσι το τελικό «γεμισμένο» μήνυμα αποτελείται από μόνον ένα (N=1) τμήμα block (φυσικά των 512 bit) :

512

				423	64
01100001	01100010	01100011	1	00…00	00…011000
a	b	c			l = 24

Για τον αλγόριθμο SHA-1, όπως είπαμε, η αρχική hash τιμή $H^{(0)}$, αποτελείται από 5 δεκαεξαδικές λέξεις των 32-bit :

$H^{(0)}_0 =$ `67452301`
$H^{(0)}_1 =$ `efcdab89`
$H^{(0)}_2 =$ `98badcfe`
$H^{(0)}_3 =$ `10325476`
$H^{(0)}_4 =$ `c3d2e1f0`

Οι 16 λέξεις των 32 bit, από τις οποίες αποτελείται το πρώτο και μοναδικό block $M^{(1)}$, από το «γεμισμένο» μήνυμα αντιστοιχούν στα τμήματα $W_0,\ldots,W_{15}$, του πίνακα – διαγράμματος :

W_0	=	61626380		W_8	=	00000000
W_1	=	00000000		W_9	=	00000000
W_2	=	00000000		W_{10}	=	00000000
W_3	=	00000000		W_{11}	=	00000000
W_4	=	00000000		W_{12}	=	00000000
W_5	=	00000000		W_{13}	=	00000000
W_6	=	00000000		W_{14}	=	00000000
W_7	=	00000000		W_{15}	=	00000018

Ο ακόλουθος πίνακας – διάγραμμα δείχνει τις δεκαεξαδικές τιμές για τις ***a***, ***b***, ***c***, ***d***, και ***e*** μετά το κάθε «πέρασμα» *t* του κύκλου "*for t = 0 to 79*" που περιγράφτηκε στο βήμα 4, στην παράγραφο Π1.6.1.2.

				a	***b***	***c***	***d***	***e***
t	=	0	:	0116fc33	67452301	7bf36ae2	98badcfe	10325476
t	=	1	:	8990536d	0116fc33	59d148c0	7bf36ae2	98badcfe
t	=	2	:	a1390f08	8990536d	c045bf0c	59d148c0	7bf36ae2
t	=	3	:	cdd8e11b	a1390f08	626414db	c045bf0c	59d148c0
t	=	4	:	cfd499de	cdd8e11b	284e43c2	626414db	c045bf0c
t	=	5	:	3fc7ca40	cfd499de	f3763846	284e43c2	626414db
t	=	6	:	993e30c1	3fc7ca40	b3f52677	f3763846	284e43c2
t	=	7	:	9e8c07d4	993e30c1	0ff1f290	b3f52677	f3763846
t	=	8	:	4b6ae328	9e8c07d4	664f8c30	0ff1f290	b3f52677
t	=	9	:	8351f929	4b6ae328	27a301f5	664f8c30	0ff1f290
t	=	10	:	fbda9e89	8351f929	12dab8ca	27a301f5	664f8c30
t	=	11	:	63188fe4	fbda9e89	60d47e4a	12dab8ca	27a301f5
t	=	12	:	4607b664	63188fe4	7ef6a7a2	60d47e4a	12dab8ca
t	=	13	:	9128f695	4607b664	18c623f9	7ef6a7a2	60d47e4a
t	=	14	:	196bee77	9128f695	1181ed99	18c623f9	7ef6a7a2
t	=	15	:	20bdd62f	196bee77	644a3da5	1181ed99	18c623f9
t	=	16	:	4e925823	20bdd62f	c65afb9d	644a3da5	1181ed99
t	=	17	:	82aa6728	4e925823	c82f758b	c65afb9d	644a3da5
t	=	18	:	dc64901d	82aa6728	d3a49608	c82f758b	c65afb9d
t	=	19	:	fd9e1d7d	dc64901d	20aa99ca	d3a49608	c82f758b
t	=	20	:	1a37b0ca	fd9e1d7d	77192407	20aa99ca	d3a49608
t	=	21	:	33a23bfc	1a37b0ca	7f67875f	77192407	20aa99ca
t	=	22	:	21283486	33a23bfc	868dec32	7f67875f	77192407
t	=	23	:	d541f12d	21283486	0ce88eff	868dec32	7f67875f
t	=	24	:	c7567dc6	d541f12d	884a0d21	0ce88eff	868dec32
t	=	25	:	48413ba4	c7567dc6	75507c4b	884a0d21	0ce88eff
t	=	26	:	be35fbd5	48413ba4	b1d59f71	75507c4b	884a0d21
t	=	27	:	4aa84d97	be35fbd5	12104ee9	b1d59f71	75507c4b
t	=	28	:	8370b52e	4aa84d97	6f8d7ef5	12104ee9	b1d59f71
t	=	29	:	c5fbaf5d	8370b52e	d2aa1365	6f8d7ef5	12104ee9
t	=	30	:	1267b407	c5fbaf5d	a0dc2d4b	d2aa1365	6f8d7ef5
t	=	31	:	3b845d33	1267b407	717eebd7	a0dc2d4b	d2aa1365
t	=	32	:	046faa0a	3b845d33	c499ed01	717eebd7	a0dc2d4b
t	=	33	:	2c0ebc11	046faa0a	cee1174c	c499ed01	717eebd7

t	=	34	:	21796ad4	2c0ebc11	811bea82	cee1174c	c499ed01
t	=	35	:	dcbbb0cb	21796ad4	4b03af04	811bea82	cee1174c
t	=	36	:	0f511fd8	dcbbb0cb	085e5ab5	4b03af04	811bea82
t	=	37	:	dc63973f	0f511fd8	f72eec32	085e5ab5	4b03af04
t	=	38	:	4c986405	dc63973f	03d447f6	f72eec32	085e5ab5
t	=	39	:	32de1cba	4c986405	f718e5cf	03d447f6	f72eec32
t	=	40	:	fc87dedf	32de1cba	53261901	f718e5cf	03d447f6
t	=	41	:	970a0d5c	fc87dedf	8cb7872e	53261901	f718e5cf
t	=	42	:	7f193dc5	970a0d5c	ff21f7b7	8cb7872e	53261901
t	=	43	:	ee1b1aaf	7f193dc5	25c28357	ff21f7b7	8cb7872e
t	=	44	:	40f28e09	ee1b1aaf	5fc64f71	25c28357	ff21f7b7
t	=	45	:	1c51e1f2	40f28e09	fb86c6ab	5fc64f71	25c28357
t	=	46	:	a01b846c	1c51e1f2	503ca382	fb86c6ab	5fc64f71
t	=	47	:	bead02ca	a01b846c	8714787c	503ca382	fb86c6ab
t	=	48	:	baf39337	bead02ca	2806e11b	8714787c	503ca382
t	=	49	:	120731c5	baf39337	afab40b2	2806e11b	8714787c
t	=	50	:	641db2ce	120731c5	eebce4cd	afab40b2	2806e11b
t	=	51	:	3847ad66	641db2ce	4481cc71	eebce4cd	afab40b2
t	=	52	:	e490436d	3847ad66	99076cb3	4481cc71	eebce4cd
t	=	53	:	27e9f1d8	e490436d	8e11eb59	99076cb3	4481cc71
t	=	54	:	7b71f76d	27e9f1d8	792410db	8e11eb59	99076cb3
t	=	55	:	5e6456af	7b71f76d	09fa7c76	792410db	8e11eb59
t	=	56	:	c846093f	5e6456af	5edc7ddb	09fa7c76	792410db
t	=	57	:	d262ff50	c846093f	d79915ab	5edc7ddb	09fa7c76
t	=	58	:	09d785fd	d262ff50	f211824f	d79915ab	5edc7ddb
t	=	59	:	3f52de5a	09d785fd	3498bfd4	f211824f	d79915ab
t	=	60	:	d756c147	3f52de5a	4275e17f	3498bfd4	f211824f
t	=	61	:	548c9cb2	d756c147	8fd4b796	4275e17f	3498bfd4
t	=	62	:	b66c020b	548c9cb2	f5d5b051	8fd4b796	4275e17f
t	=	63	:	6b61c9e1	b66c020b	9523272c	f5d5b051	8fd4b796
t	=	64	:	19dfa7ac	6b61c9e1	ed9b0082	9523272c	f5d5b051
t	=	65	:	101655f9	19dfa7ac	5ad87278	ed9b0082	9523272c
t	=	66	:	0c3df2b4	101655f9	0677e9eb	5ad87278	ed9b0082
t	=	67	:	78dd4d2b	0c3df2b4	4405957e	0677e9eb	5ad87278
t	=	68	:	497093c0	78dd4d2b	030f7cad	4405957e	0677e9eb
t	=	69	:	3f2588c2	497093c0	de37534a	030f7cad	4405957e
t	=	70	:	c199f8c7	3f2588c2	125c24f0	de37534a	030f7cad
t	=	71	:	39859de7	c199f8c7	8fc96230	125c24f0	de37534a
t	=	72	:	edb42de4	39859de7	f0667e31	8fc96230	125c24f0
t	=	73	:	11793f6f	edb42de4	ce616779	f0667e31	8fc96230
t	=	74	:	5ee76897	11793f6f	3b6d0b79	ce616779	f0667e31
t	=	75	:	63f7dab7	5ee76897	c45e4fdb	3b6d0b79	ce616779
t	=	76	:	a079b7d9	63f7dab7	d7b9da25	c45e4fdb	3b6d0b79
t	=	77	:	860d21cc	a079b7d9	d8fdf6ad	d7b9da25	c45e4fdb
t	=	78	:	5738d5e1	860d21cc	681e6df6	d8fdf6ad	d7b9da25
t	=	79	:	42541b35	5738d5e1	21834873	681e6df6	d8fdf6ad

Με αυτό τελειώνει η επεξεργασία του πρώτου και μοναδικού τμήματος (block) $M^{(1)}$, από το οποίο αποτελείται το μήνυμα. Η τελική τιμή hash τιμή $H^{(1)}$, δίνεται από :

$H_0^{(1)}$	=	67452301	+	42541b35	=	**a9993e36**
$H_1^{(1)}$	=	efcdab89	+	5738d5e1	=	**4706816a**
$H_2^{(1)}$	=	98badcfe	+	21834873	=	**ba3e2571**
$H_3^{(1)}$	=	10325476	+	681e6df6	=	**7850c26c**
$H_4^{(1)}$	=	c3d2e1f0	+	d8fdf6ad	=	**9cd0d89d**

Το αποτέλεσμα των 160-bit, της τελικής σύνοψης και υπογραφής του μηνύματος, δίνεται από τη συνένωση αυτών των λέξεων :

a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d.

Π1.Α.2 SHA-1 Παράδειγμα Μηνύματος πολλαπλών τμημάτων (Multi-block message)

Έστω ότι το μήνυμα *M*, των 448-bit ($l = 448 = 56$ χαρακτήρες x 8 bit) μιας ASCII συμβολοσειράς είναι το εξής :

"**abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq**".

Το μήνυμα «γεμίζεται» προσθέτοντας πρώτα το bit "1", ακολουθούμενο από 511 μηδενικά bits – "0", και τέλος από την δεκαεξαδική τιμή $(00000000\ 000001c0)_{hex}$, (δηλ. τις 2 λέξεις των 32-bit, που αντιστοιχούν στην δεκαεξαδική τιμή του δεκαδικού αριθμού 448, που είναι το μήκος της συμβολοσειράς σε bits).
Έτσι το τελικά διαμορφωμένο μήνυμα μετά το «γέμισμα» αποτελείται από 1024 bits, δηλ από δύο blocks των 512 bits το καθένα, κι επομένως $N = 2$.

Για τον αλγόριθμο SHA-1, όπως ήδη έχουμε ξανά αναφέρει, η αρχική hash τιμή $H^{(0)}$, αποτελείται από 5 δεκαεξαδικές λέξεις των 32-bit :

$H^{(0)}_0 = 67452301$
$H^{(0)}_1 = efcdab89$
$H^{(0)}_2 = 98badcfe$
$H^{(0)}_3 = 10325476$
$H^{(0)}_4 = c3d2e1f0$

Οι 16 λέξεις των 32 bit, από τις οποίες αποτελείται το πρώτο block $M^{(1)}$, από το «γεμισμένο» μήνυμα αντιστοιχούν στα τμήματα $W_0,\ldots,W_{15}$, του πίνακα – διαγράμματος :

W_0	=	61626364		W_8	=	696a6b6c
W_1	=	62636465		W_9	=	6a6b6c6d
W_2	=	63646566		W_{10}	=	6b6c6d6e
W_3	=	64656667		W_{11}	=	6c6d6e6f
W_4	=	65666768		W_{12}	=	6d6e6f70
W_5	=	66676869		W_{13}	=	6e6f7071
W_6	=	6768696a		W_{14}	=	80000000
W_7	=	68696a6b		W_{15}	=	00000000

Ο ακόλουθος πίνακας – διάγραμμα δείχνει τις δεκαεξαδικές τιμές για τις ***a***, ***b***, ***c***, ***d***, και ***e*** μετά το κάθε «πέρασμα» *t* του κύκλου "*for t = 0 to 79*" που περιγράφτηκε στο βήμα 4, στην παράγραφο Π1.6.1.2.

				a	***b***	***c***	***d***	***e***
t	=	0	:	0116fc17	67452301	7bf36ae2	98badcfe	10325476
t	=	1	:	ebf3b452	0116fc17	59d148c0	7bf36ae2	98badcfe
t	=	2	:	5109913a	ebf3b452	c045bf05	59d148c0	7bf36ae2

t	=	3	:	2c4f6eac	5109913a	bafced14	c045bf05	59d148c0
t	=	4	:	33f4ae5b	2c4f6eac	9442644e	bafced14	c045bf05
t	=	5	:	96b85189	33f4ae5b	0b13dbab	9442644e	bafced14
t	=	6	:	db04cb58	96b85189	ccfd2b96	0b13dbab	9442644e
t	=	7	:	45833f0f	db04cb58	65ae1462	ccfd2b96	0b13dbab
t	=	8	:	c565c35e	45833f0f	36c132d6	65ae1462	ccfd2b96
t	=	9	:	6350afda	c565c35e	d160cfc3	36c132d6	65ae1462
t	=	10	:	8993ea77	6350afda	b15970d7	d160cfc3	36c132d6
t	=	11	:	e19ecaa2	8993ea77	98d42bf6	b15970d7	d160cfc3
t	=	12	:	8603481e	e19ecaa2	e264fa9d	98d42bf6	b15970d7
t	=	13	:	32f94a85	8603481e	b867b2a8	e264fa9d	98d42bf6
t	=	14	:	b2e7a8be	32f94a85	a180d207	b867b2a8	e264fa9d
t	=	15	:	42637e39	b2e7a8be	4cbe52a1	a180d207	b867b2a8
t	=	16	:	6b068048	42637e39	acb9ea2f	4cbe52a1	a180d207
t	=	17	:	426b9c35	6b068048	5098df8e	acb9ea2f	4cbe52a1
t	=	18	:	944b1bd1	426b9c35	1ac1a012	5098df8e	acb9ea2f
t	=	19	:	6c445652	944b1bd1	509ae70d	1ac1a012	5098df8e
t	=	20	:	95836da5	6c445652	6512c6f4	509ae70d	1ac1a012
t	=	21	:	09511177	95836da5	9b111594	6512c6f4	509ae70d
t	=	22	:	e2b92dc4	09511177	6560db69	9b111594	6512c6f4
t	=	23	:	fd224575	e2b92dc4	c254445d	6560db69	9b111594
t	=	24	:	eeb82d9a	fd224575	38ae4b71	c254445d	6560db69
t	=	25	:	5a142c1a	eeb82d9a	7f48915d	38ae4b71	c254445d
t	=	26	:	2972f7c7	5a142c1a	bbae0b66	7f48915d	38ae4b71
t	=	27	:	d526a644	2972f7c7	96850b06	bbae0b66	7f48915d
t	=	28	:	e1122421	d526a644	ca5cbdf1	96850b06	bbae0b66
t	=	29	:	05b457b2	e1122421	3549a991	ca5cbdf1	96850b06
t	=	30	:	a9c84bec	05b457b2	78448908	3549a991	ca5cbdf1
t	=	31	:	52e31f60	a9c84bec	816d15ec	78448908	3549a991
t	=	32	:	5af3242c	52e31f60	2a7212fb	816d15ec	78448908
t	=	33	:	31c756a9	5af3242c	14b8c7d8	2a7212fb	816d15ec
t	=	34	:	e9ac987c	31c756a9	16bcc90b	14b8c7d8	2a7212fb
t	=	35	:	ab7c32ee	e9ac987c	4c71d5aa	16bcc90b	14b8c7d8
t	=	36	:	5933fc99	ab7c32ee	3a6b261f	4c71d5aa	16bcc90b
t	=	37	:	43f87ae9	5933fc99	aadf0cbb	3a6b261f	4c71d5aa
t	=	38	:	24957f22	43f87ae9	564cff26	aadf0cbb	3a6b261f
t	=	39	:	adeb7478	24957f22	50fe1eba	564cff26	aadf0cbb
t	=	40	:	d70e5010	adeb7478	89255fc8	50fe1eba	564cff26
t	=	41	:	79bcfb08	d70e5010	2b7add1e	89255fc8	50fe1eba
t	=	42	:	f9bcb8de	79bcfb08	35c39404	2b7add1e	89255fc8
t	=	43	:	633e9561	f9bcb8de	1e6f3ec2	35c39404	2b7add1e
t	=	44	:	98c1ea64	633e9561	be6f2e37	1e6f3ec2	35c39404
t	=	45	:	c6ea241e	98c1ea64	58cfa558	be6f2e37	1e6f3ec2
t	=	46	:	a2ad4f02	c6ea241e	26307a99	58cfa558	be6f2e37
t	=	47	:	c8a69090	a2ad4f02	b1ba8907	26307a99	58cfa558
t	=	48	:	88341600	c8a69090	a8ab53c0	b1ba8907	26307a99
t	=	49	:	7e846f58	88341600	3229a424	a8ab53c0	b1ba8907
t	=	50	:	86e358ba	7e846f58	220d0580	3229a424	a8ab53c0
t	=	51	:	8d2e76c8	86e358ba	1fa11bd6	220d0580	3229a424
t	=	52	:	ce892e10	8d2e76c8	a1b8d62e	1fa11bd6	220d0580
t	=	53	:	edea95b1	ce892e10	234b9db2	a1b8d62e	1fa11bd6
t	=	54	:	36d1230a	edea95b1	33a24b84	234b9db2	a1b8d62e
t	=	55	:	776c3910	36d1230a	7b7aa56c	33a24b84	234b9db2
t	=	56	:	a681b723	776c3910	8db448c2	7b7aa56c	33a24b84
t	=	57	:	ac0a794f	a681b723	1ddb0e44	8db448c2	7b7aa56c

t	=	58	:	f03d3782	ac0a794f	e9a06dc8	1ddb0e44	8db448c2
t	=	59	:	9ef775c3	f03d3782	eb029e53	e9a06dc8	1ddb0e44
t	=	60	:	36254b13	9ef775c3	bc0f4de0	eb029e53	e9a06dc8
t	=	61	:	4080d4dc	36254b13	e7bddd70	bc0f4de0	eb029e53
t	=	62	:	2bfaf7a8	4080d4dc	cd8952c4	e7bddd70	bc0f4de0
t	=	63	:	513f9ca0	2bfaf7a8	10203537	cd8952c4	e7bddd70
t	=	64	:	e5895c81	513f9ca0	0afebdea	10203537	cd8952c4
t	=	65	:	1037d2d5	e5895c81	144fe728	0afebdea	10203537
t	=	66	:	14a82da9	1037d2d5	79625720	144fe728	0afebdea
t	=	67	:	6d17c9fd	14a82da9	440df4b5	79625720	144fe728
t	=	68	:	2c7b07bd	6d17c9fd	452a0b6a	440df4b5	79625720
t	=	69	:	fdf6efff	2c7b07bd	5b45f27f	452a0b6a	440df4b5
t	=	70	:	112b96e3	fdf6efff	4b1ec1ef	5b45f27f	452a0b6a
t	=	71	:	84065712	112b96e3	ff7dbbff	4b1ec1ef	5b45f27f
t	=	72	:	ab89fb71	84065712	c44ae5b8	ff7dbbff	4b1ec1ef
t	=	73	:	c5210e35	ab89fb71	a10195c4	c44ae5b8	ff7dbbff
t	=	74	:	352d9f4b	c5210e35	6ae27edc	a10195c4	c44ae5b8
t	=	75	:	1a0e0e0a	352d9f4b	7148438d	6ae27edc	a10195c4
t	=	76	:	d0d47349	1a0e0e0a	cd4b67d2	7148438d	6ae27edc
t	=	77	:	ad38620d	d0d47349	86838382	cd4b67d2	7148438d
t	=	78	:	d3ad7c25	ad38620d	74351cd2	86838382	cd4b67d2
t	=	79	:	8ce34517	d3ad7c25	6b4e1883	74351cd2	86838382

Με αυτό τελειώνει η επεξεργασία του πρώτου block $M^{(1)}$ του μηνύματος.
Η πρώτη ενδιάμεση (και τελευταία) hash τιμή $H^{(1)}$, υπολογίζεται σε :

$H^{(0)}_0$ = 67452301 + 8ce34517 = f4286818
$H^{(0)}_1$ = efcdab89 + d3ad7c25 = c37b27ae
$H^{(0)}_2$ = 98badcfe + 6b4e1883 = 0408f581
$H^{(0)}_3$ = 10325476 + 74351cd2 = 84677148
$H^{(0)}_4$ = c3d2e1f0 + 86838382 = 4a566572

Οι 16 λέξεις των 32 bit, από τις οποίες αποτελείται το δεύτερο block $M^{(2)}$, από το «γεμισμένο» μήνυμα, αντιστοιχούν στα τμήματα $W_0,\ldots,W_{15}$, του πίνακα – διαγράμματος :

W_0	=	00000000		W_8	=	00000000
W_1	=	00000000		W_9	=	00000000
W_2	=	00000000		W_{10}	=	00000000
W_3	=	00000000		W_{11}	=	00000000
W_4	=	00000000		W_{12}	=	00000000
W_5	=	00000000		W_{13}	=	00000000
W_6	=	00000000		W_{14}	=	00000000
W_7	=	00000000		W_{15}	=	000001c0

Ο ακόλουθος πίνακας – διάγραμμα δείχνει τις δεκαεξαδικές τιμές για τις ***a***, ***b***, ***c***, ***d***, και ***e*** μετά το κάθε «πέρασμα» *t* του κύκλου "*for t = 0 to 79*" που περιγράφτηκε στο βήμα 4, στην παράγραφο Π1.6.1.2.

				a	***b***	***c***	***d***	***e***
t	=	0	:	2df257e9	f4286818	b0dec9eb	0408f581	84677148
t	=	1	:	4d3dc58f	2df257e9	3d0a1a06	b0dec9eb	0408f581

t	=	2	:	c352bb05	4d3dc58f	4b7c95fa	3d0a1a06	b0dec9eb
t	=	3	:	eef743c6	c352bb05	d34f7163	4b7c95fa	3d0a1a06
t	=	4	:	41e34277	eef743c6	70d4aec1	d34f7163	4b7c95fa
t	=	5	:	5443915c	41e34277	bbbdd0f1	70d4aec1	d34f7163
t	=	6	:	e7fa0377	5443915c	d078d09d	bbbdd0f1	70d4aec1
t	=	7	:	c6946813	e7fa0377	1510e457	d078d09d	bbbdd0f1
t	=	8	:	fdde1de1	c6946813	f9fe80dd	1510e457	d078d09d
t	=	9	:	b8538aca	fdde1de1	f1a51a04	f9fe80dd	1510e457
t	=	10	:	6ba94f63	b8538aca	7f778778	f1a51a04	f9fe80dd
t	=	11	:	43a2792f	6ba94f63	ae14e2b2	7f778778	f1a51a04
t	=	12	:	fecd7bbf	43a2792f	daea53d8	ae14e2b2	7f778778
t	=	13	:	a2604ca8	fecd7bbf	d0e89e4b	daea53d8	ae14e2b2
t	=	14	:	258b0baa	a2604ca8	ffb35eef	d0e89e4b	daea53d8
t	=	15	:	d9772360	258b0baa	2898132a	ffb35eef	d0e89e4b
t	=	16	:	5507db6e	d9772360	8962c2ea	2898132a	ffb35eef
t	=	17	:	a51b58bc	5507db6e	365dc8d8	8962c2ea	2898132a
t	=	18	:	c2eb709f	a51b58bc	9541f6db	365dc8d8	8962c2ea
t	=	19	:	d8992153	c2eb709f	2946d62f	9541f6db	365dc8d8
t	=	20	:	37482f5f	d8992153	f0badc27	2946d62f	9541f6db
t	=	21	:	ee8700bd	37482f5f	f6264854	f0badc27	2946d62f
t	=	22	:	9ad594b9	ee8700bd	cdd20bd7	f6264854	f0badc27
t	=	23	:	8fbaa5b9	9ad594b9	7ba1c02f	cdd20bd7	f6264854
t	=	24	:	88fb5867	8fbaa5b9	66b5652e	7ba1c02f	cdd20bd7
t	=	25	:	eec50521	88fb5867	63eea96e	66b5652e	7ba1c02f
t	=	26	:	50bce434	eec50521	e23ed619	63eea96e	66b5652e
t	=	27	:	5c416daf	50bce434	7bb14148	e23ed619	63eea96e
t	=	28	:	2429be5f	5c416daf	142f390d	7bb14148	e23ed619
t	=	29	:	0a2fb108	2429be5f	d7105b6b	142f390d	7bb14148
t	=	30	:	17986223	0a2fb108	c90a6f97	d7105b6b	142f390d
t	=	31	:	8a4af384	17986223	028bec42	c90a6f97	d7105b6b
t	=	32	:	6b629993	8a4af384	c5e61888	028bec42	c90a6f97
t	=	33	:	f15f04f3	6b629993	2292bce1	c5e61888	028bec42
t	=	34	:	295cc25b	f15f04f3	dad8a664	2292bce1	c5e61888
t	=	35	:	696da404	295cc25b	fc57c13c	dad8a664	2292bce1
t	=	36	:	cef5ae12	696da404	ca573096	fc57c13c	dad8a664
t	=	37	:	87d5b80c	cef5ae12	1a5b6901	ca573096	fc57c13c
t	=	38	:	84e2a5f2	87d5b80c	b3bd6b84	1a5b6901	ca573096
t	=	39	:	03bb6310	84e2a5f2	21f56e03	b3bd6b84	1a5b6901
t	=	40	:	c2d8f75f	03bb6310	a138a97c	21f56e03	b3bd6b84
t	=	41	:	bfb25768	c2d8f75f	00eed8c4	a138a97c	21f56e03
t	=	42	:	28589152	bfb25768	f0b63dd7	00eed8c4	a138a97c
t	=	43	:	ec1d3d61	28589152	2fec95da	f0b63dd7	00eed8c4
t	=	44	:	3caed7af	ec1d3d61	8a162454	2fec95da	f0b63dd7
t	=	45	:	c3d033ea	3caed7af	7b074f58	8a162454	2fec95da
t	=	46	:	7316056a	c3d033ea	cf2bb5eb	7b074f58	8a162454
t	=	47	:	46f93b68	7316056a	b0f40cfa	cf2bb5eb	7b074f58
t	=	48	:	dc8e7f26	46f93b68	9cc5815a	b0f40cfa	cf2bb5eb
t	=	49	:	850d411c	dc8e7f26	11be4eda	9cc5815a	b0f40cfa
t	=	50	:	7e4672c0	850d411c	b7239fc9	11be4eda	9cc5815a
t	=	51	:	89fbd41d	7e4672c0	21435047	b7239fc9	11be4eda
t	=	52	:	1797e228	89fbd41d	1f919cb0	21435047	b7239fc9
t	=	53	:	431d65bc	1797e228	627ef507	1f919cb0	21435047
t	=	54	:	2bdbb8cb	431d65bc	05e5f88a	627ef507	1f919cb0
t	=	55	:	6da72e7f	2bdbb8cb	10c7596f	05e5f88a	627ef507
t	=	56	:	a8495a9b	6da72e7f	caf6ee32	10c7596f	05e5f88a

t	=	57	:	e785655a	a8495a9b	db69cb9f	caf6ee32	10c7596f
t	=	58	:	5b086c42	e785655a	ea1256a6	db69cb9f	caf6ee32
t	=	59	:	a65818f7	5b086c42	b9e15956	ea1256a6	db69cb9f
t	=	60	:	7aab101b	a65818f7	96c21b10	b9e15956	ea1256a6
t	=	61	:	93614c9c	7aab101b	e996063d	96c21b10	b9e15956
t	=	62	:	f66d9bf4	93614c9c	deaac406	e996063d	96c21b10
t	=	63	:	d504902b	f66d9bf4	24d85327	deaac406	e996063d
t	=	64	:	60a9da62	d504902b	3d9b66fd	24d85327	deaac406
t	=	65	:	8b687819	60a9da62	f541240a	3d9b66fd	24d85327
t	=	66	:	083e90c3	8b687819	982a7698	f541240a	3d9b66fd
t	=	67	:	f6226bbf	083e90c3	62da1e06	982a7698	f541240a
t	=	68	:	76c0563b	f6226bbf	c20fa430	62da1e06	982a7698
t	=	69	:	989dd165	76c0563b	fd889aef	c20fa430	62da1e06
t	=	70	:	8b2c7573	989dd165	ddb0158e	fd889aef	c20fa430
t	=	71	:	ae1b8e7b	8b2c7573	66277459	ddb0158e	fd889aef
t	=	72	:	ca1840de	ae1b8e7b	e2cb1d5c	66277459	ddb0158e
t	=	73	:	16f3babb	ca1840de	eb86e39e	e2cb1d5c	66277459
t	=	74	:	d28d83ad	16f3babb	b2861037	eb86e39e	e2cb1d5c
t	=	75	:	6bc02dfe	d28d83ad	c5bceeae	b2861037	eb86e39e
t	=	76	:	d3a6e275	6bc02dfe	74a360eb	c5bceeae	b2861037
t	=	77	:	da955482	d3a6e275	9af00b7f	74a360eb	c5bceeae
t	=	78	:	58c0aac0	da955482	74e9b89d	9af00b7f	74a360eb
t	=	79	:	906fd62c	58c0aac0	b6a55520	74e9b89d	9af00b7f

Με αυτό τελειώνει η επεξεργασία του δεύτερου και τελευταίου τμήματος (block) $M^{(2)}$, του μηνύματος. Η δεύτερη και τελική τιμή hash τιμή $H^{(2)}$, δίνεται από :

$H_0^{(2)}$	=	f4286818	+	906fd62c	=	**84983e44**
$H_1^{(2)}$	=	c37b27ae	+	58c0aac0	=	**1c3bd26e**
$H_2^{(2)}$	=	0408f581	+	b6a55520	=	**baae4aa1**
$H_3^{(2)}$	=	84677148	+	74e9b89d	=	**f95129e5**
$H_4^{(2)}$	=	4a566572	+	9af00b7f	=	**e54670f1**

Το αποτέλεσμα των 160-bit, της τελικής σύνοψης και υπογραφής του μηνύματος, δίνεται από τη συνένωση αυτών των λέξεων :

84983e44 1c3bd26e baae4aa1 f95129e5 e54670f1

Π1.Α.3 SHA-1 Αναφορά αποτελέσματος σε παράδειγμα Μηνύματος Μεγάλου Μήκους

Έστω ότι το μήνυμα M, αποτελείται από μια ASCII συμβολοσειρά 1.000.000 επαναλαμβανόμενων χαρακτήρων του γράμματος «a» (πρόκειται δηλαδή για 8.000.000 bit). Το αποτέλεσμα των 160-bit, της τελικής σύνοψης και υπογραφής του μηνύματος είναι :

34aa973c d4c4daa4 f61eeb2b dbad2731 6534016f

ΠΑΡΑΡΤΗΜΑ Π2

ΠΡΟΤΕΙΝΟΜΕΝΟΣ Πίνακας Ελληνικών ASCII – ΕΛΟΤ 928 (MS) (θέσεις 128 - 255)

Dec	Hex	ASCII	Dec	Hex	Ascii	Dec	Hex	Ascii	Dec	Hex	Ascii
128	80	€	160	A0	NBSP	192	C0	ΐ	224	E0	ΰ
129	81		161	A1	΅	193	C1	Α	225	E1	α
130	82		162	A2	Ά	194	C2	Β	226	E2	β
131	83		163	A3	£	195	C3	Γ	227	E3	γ
132	84		164	A4	¤	196	C4	Δ	228	E4	δ
133	85		165	A5	¥	197	C5	Ε	229	E5	ε
134	86		166	A6	¦	198	C6	Ζ	230	E6	ζ
135	87		167	A7	§	199	C7	Η	231	E7	η
136	88		168	A8	¨	200	C8	Θ	232	E8	θ
137	89		169	A9	©	201	C9	Ι	233	E9	ι
138	8A		170	AA	□	202	CA	Κ	234	EA	κ
139	8B		171	AB	«	203	CB	Λ	235	EB	λ
140	8C		172	AC	¬	204	CC	Μ	236	EC	μ
141	8D		173	AD		205	CD	Ν	237	ED	ν
142	8E		174	AE	®	206	CE	Ξ	238	EE	ξ
143	8F		175	AF	―	207	CF	Ο	239	EF	ο
144	90		176	B0	°	208	D0	Π	240	F0	π
145	91		177	B1	±	209	D1	Ρ	241	F1	ρ
146	92		178	B2	²	210	D2		242	F2	ς
147	93		179	B3	³	211	D3	Σ	243	F3	σ
148	94		180	B4	΄	212	D4	Τ	244	F4	τ
149	95		181	B5	μ	213	D5	Υ	245	F5	υ
150	96		182	B6	¶	214	D6	Φ	246	F6	φ
151	97		183	B7	·	215	D7	Χ	247	F7	χ
152	98		184	B8	Έ	216	D8	Ψ	248	F8	ψ
153	99		185	B9	Ή	217	D9	Ω	249	F9	ω
154	9A		186	BA	Ί	218	DA	Ϊ	250	FA	ϊ
155	9B		187	BB	»	219	DB	Ϋ	251	FB	ϋ
156	9C		188	BC	Ό	220	DC	ά	252	FC	ό
157	9D		189	BD	½	221	DD	έ	253	FD	ύ
158	9E		190	BE	Ύ	222	DE	ή	254	FE	ώ
159	9F		191	BF	Ώ	223	DF	ί	255	FF	

Ο Πίνακας ΕΛΟΤ 928, όπως διαμορφώθηκε με τις αλλαγές που έγιναν από την MICROSOFT, στα WINDOWS 3.1 και χρησιμοποιείται στα 8-bit fonts. Είναι γνωστός επίσης ως διεθνές standard : iso8859-7, ISO 8859-7, ecma118, elot928, iso88597, iso885971987, isoir126, κλπ. Τα Ελληνικά που υποστηρίζει η Version 3.1 των WINDOWS της MICROSOFT, είναι αυτά του ΕΛΟΤ 928 με 4 μόνο διαφορές, που στην συντριπτική πλειοψηφία των περιπτώσεων δεν δημιουργούν κανένα πρόβλημα. Στο MS 928 - ας το ονομάσουμε έτσι, για να το ξεχωρίζουμε από το κανονικό ΕΛΟΤ 928 - η MICROSOFT κατήργησε την δασεία και την ψιλή στις θέσεις 161 και 162, και στην θέση τους έβαλε τα διαλυτικά με τόνο (΅)και το τονισμένο κεφαλαίο (Ά) αντίστοιχα. Στο κανονικό ΕΛΟΤ 928, αυτά τα σύμβολα ευρίσκονται στις θέσεις 181 και 182, στις οποίες τώρα το MS 928 βάζει το μαθηματικό (μ) και το σύμβολο αλλαγής παραγράφου (¶) αντίστοιχα.

Τα μέλη της Επιτροπής :

Καψάλης Χρήστος – Πρόεδρος

Σταφυλοπάτης Ανδρέας-Γεώργιος

Παναγιωτόπουλος Τάκης

Γυφτάκη Μαρία

Ζαφειρόπουλος Παναγιώτης