Οδηγίες για την επιβεβαίωση της εγκυρότητάς των ψηφιακών υπογραφών των αρχείων και της εγκυρότητάς των αρχείων ZIP

Α) Οδηγίες για την επιβεβαίωση της εγκυρότητάς των ψηφιακών υπογραφών των αρχείων

Σε περίπτωση που κάποιος επιθυμεί να προβεί σε επιβεβαίωση της εγκυρότητάς των ψηφιακών υπογραφών των εγγράφων σε υπολογιστή με λειτουργικό σύστημα Windows, ακολουθείται η παρακάτω διαδικασία:

1) στην σελίδα https://pki.ermis.gov.gr/repository.html επιλέγουμε με δεξί κλικ την αποθήκευση στο υπολογιστή μας (save target as) του Πιστοποιητικού Πρωτεύουσας Αρχής Πιστοποίησης ermis, σε μορφή DER ή Base64.

2) Εντοπίζουμε το αρχείο ermis_root_64.cer (η το αρχείο ermis_root_der.cer) στον φάκελο του υπολογιστή μας στον οποίο το αποθηκεύσαμε στο βήμα 1 και με δεξί κλικ επιλέγουμε «install certificate» (εγκατάσταση πιστοποιητικού)

3) Στην επόμενη οθόνη επιλέγουμε «next» και στην αμέσως επόμενη επιλέγουμε«Place all certificates in the following store» και πατάμε «Browse»

4) Στην επόμενη οθόνη επιλέγουμε «Trusted Root Certification Authorities»

5) Αφού έχουμε επιλέξει «Trusted Root Certification Authorities» πατάμε“Next” και μετά “Finish”

6) Τέλος στην ερώτηση των windows εάν θέλουμε να προσθέσουμε το συγκεκριμένο πιστοποιητικό στην λίστα των Trusted Root Certification Authorities επιλέγουμε «Yes»

Σημείωση: Για την επιβεβαίωση της εγκυρότητάς των ψηφιακών υπογραφών των συνημμένων αρχείων απαιτείται η έκδοση Acrobat Reader X (10.1.0) ή νεότερη. Σε περίπτωση που το πρόγραμμα Acrobat Reader X (10.1.0) συνεχίζει να χαρακτηρίζει την ψηφιακή υπογραφή ως άγνωστη: «Signature Validity is unknown». Ακολουθούμε τα ακόλουθα βήματα:

1) Από το μενού επιλέγουμε Edit -> Preferences. Στο επόμενο παράθυρο από τη λίστα των categories επιλέγουμε «security» και στην εμφανιζόμενη καρτέλα επιλέγουμε «Advanced Preferences».

2) Πηγαίνουμε στην καρτέλα (Tab) «Windows Integration» και επιλέγουμε και τις 2 ακόλουθες επιλογές: «Validating Signatures» και «Validating Certified Documents» και πατάμε «Ok»

3) Στην επόμενη καρτέλα πατάμε επίσης «Ok».

4) Κλείνουμε το πρόγραμμα Acrobat και ανοίγουμε ξανά το έγγραφο.

Οι παραλήπτες των αρχείων σε μορφή MS WORD και EXCEL μπορούν να επιβεβαιώσουν την ψηφιακή υπογραφή των αρχείων αυτών μεταβαίνοντας στις επιλογές του αρχείου: **Tools / options / security / Digital Signatures / View Certificate**

Β) Οδηγίες για την επιβεβαίωση της εγκυρότητάς των αρχείων ZIP

Σε περίπτωση που κάποιος επιθυμεί να προβεί σε επιβεβαίωση της εγκυρότητάς των αρχείων zip μπορεί να χρησιμοποιήσει το αρχείο από τον σύνδεσμο «Επαλήθευση Zip αρχείων». Το συγκεκριμένο αρχείο περιέχει το αποτέλεσμα του αλγορίθμου SHA1 για κάθε αρχείο zip. Αυτό εξασφαλίζει ότι οποιαδήποτε αλλαγή έχει πραγματοποιηθεί στο αρχείο zip θα γίνει αντιληπτή καθώς ο αλγόριθμος SHA1 θα παράγει διαφορετικό αποτέλεσμα.
Για την επιβεβαίωση της εγκυρότητάς των αρχείων zip μπορεί να χρησιμοποιηθεί η παρακάτω διαδικασία:

1) Επιβεβαιώνουμε την εγκυρότητα του αρχείου που διαβάζετε αυτή τη στιγμή μέσω της συνημμένης ψηφιακής υπογραφής (Βλέπε παράγραφο «Οδηγίες για την επιβεβαίωση της εγκυρότητας των ψηφιακών υπογραφών των αρχείων»)

2) Χρησιμοποιούμε ένα οποιοδήποτε δωρεάν πρόγραμμα παραγωγής SHA1 από το internet (π.χ. το MD5 & SHA-1 Checksum Utility)

3) «εισάγουμε» το αρχείο zip που θέλουμε να επαληθεύσουμε στο πρόγραμμα παραγωγής SHA-1 και το πρόγραμμα παραγωγής SHA-1 παράγει ένα κωδικό για το συγκεκριμένο αρχείο zip

4) Επαληθεύουμε το αποτέλεσμα (κωδικό) του αλγορίθμου SHA1 από το βήμα 3 με τους ακόλουθους κωδικούς:

   Για το (SHA1): ΤΕΥΧΗ ΔΙΑΓΩΝΙΣΜΟΥ_ΚΤΙΜΑ_16.zip
   ο κωδικός είναι: F9C5A13B6576DFBB5DEF67B30F80D23A674F2358

   Για το (SHA1): ΛΟΙΠΑ ΣΤΟΙΧΕΙΑ ΤΟΥ ΦΑΚΕΛΟΥ ΤΟΥ ΕΡΓΟΥ_ΚΤΙΜΑ_16.zip
   ο κωδικός είναι: 69D51B85F0ECD8B2E5810F0FAF6ABF66722DD109

5) Οι δύο κωδικοί θα πρέπει να είναι ίδιοι.