

Εθνική Πύλη www.ermis.gov.gr

Εγκατάσταση Πιστοποιητικών
Αρχής Πιστοποίησης Ελληνικού Δημοσίου

Έκδοση 1.3

Πίνακας Περιεχομένων

1.	<u>ΕΙΣΑΓΩΓΗ</u>	<u>3</u>
2.	<u>ΠΡΟΕΤΟΙΜΑΣΙΑ ΕΓΚΑΤΑΣΤΑΣΗΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΤΗΣ ΑΠΕΔ</u>	<u>3</u>
2.1	ΕΓΚΑΤΑΣΤΑΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΠΡΩΤΕΥΟΥΣΑΣ ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ	4
2.2	ΕΓΚΑΤΑΣΤΑΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΤΗΣ ΥΠΟΚΕΙΜΕΝΗΣ ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΣΤΟΝ INTERNET EXPLORER	10
3.	<u>ΕΓΚΑΤΑΣΤΑΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΧΡΟΝΟΣΗΜΑΝΣΗΣ (TSA) ΤΗΣ ΑΠΕΔ</u>	<u>13</u>
4.	<u>ΠΡΟΕΤΟΙΜΑΣΙΑ ΦΥΛΛΟΜΕΤΡΗΤΗ (WEB BROWSER)</u>	<u>13</u>

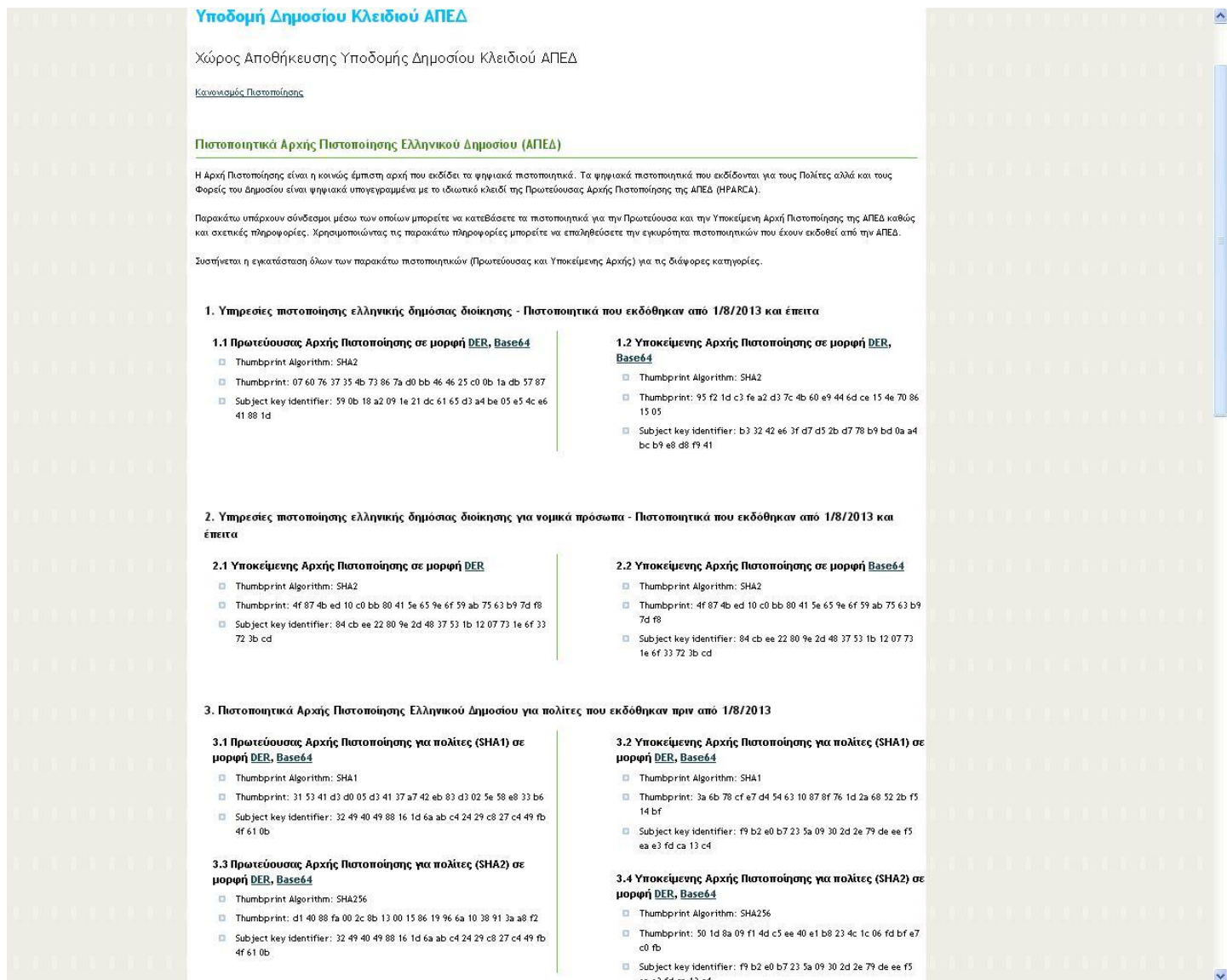
1. Εισαγωγή

Το παρόν εγχειρίδιο οδηγιών αφορά τους τελικούς χρήστες της Εθνικής πύλης ΕΡΜΗΣ (www.ermis.gov.gr), που θέλουν να εκδώσουν και να χρησιμοποιήσουν ψηφιακά πιστοποιητικά τα οποία έχουν εκδοθεί από την [Αρχή Πιστοποίησης του Ελληνικού Δημοσίου \(ΑΠΕΔ\)](#). Στο παρόν εγχειρίδιο περιγράφεται η διαδικασία εγκατάστασης των απαραίτητων πιστοποιητικών της ΑΠΕΔ, όπως των πιστοποιητικών ασφαλούς χρονοσήμανσης. Επίσης, περιγράφονται οι ρυθμίσεις που θα πρέπει να γίνουν στον φυλλομετρητή (web browser) προκειμένου να καταστεί δυνατή η έκδοση των προσωπικών ψηφιακών πιστοποιητικών του τελικού χρήστη.

2. Προετοιμασία εγκατάστασης των πιστοποιητικών της ΑΠΕΔ

Τα πιστοποιητικά της Πρωτεύουσας Αρχής Πιστοποίησης (ΠΑΠ ή Root CA) και της Υποκείμενης Αρχής Πιστοποίησης (ΥΠΑΠ ή Issuing CA) που θα πρέπει να εγκατασταθούν στον φυλλομετρητή, βρίσκονται στην ιστοσελίδα <https://pki.ermis.gov.gr/repository.html> όπως φαίνεται στην Εικόνα 1. Για λόγους διασφάλισης της ομαλότητας εγκατάστασης των πιστοποιητικών σε ΑΔΔΥ (usb token ή έξυπνη κάρτα), θα πρέπει να χρησιμοποιηθεί αποκλειστικά ως browser, ο Internet Explorer στη διαδικασία έκδοσης των πιστοποιητικών (έκδοση πιστοποιητικών σκληρής αποθήκευσης). Στην περίπτωση πιστοποιητικών χαλαρής αποθήκευσης θα μπορούσε εναλλακτικά του Internet Explorer να χρησιμοποιηθεί Firefox Mozilla. Η συγκεκριμένη διαδικασία περιγράφεται αναλυτικά στις επόμενες ενότητες.

Σημαντική σημείωση: Για τις παρακάτω διαδικασίες εγκατάστασης των εργαλείων όπως και των ψηφιακών πιστοποιητικών θα χρειαστεί να έχετε δικαιώματα διαχειριστή (Administrator) στον υπολογιστή σας.

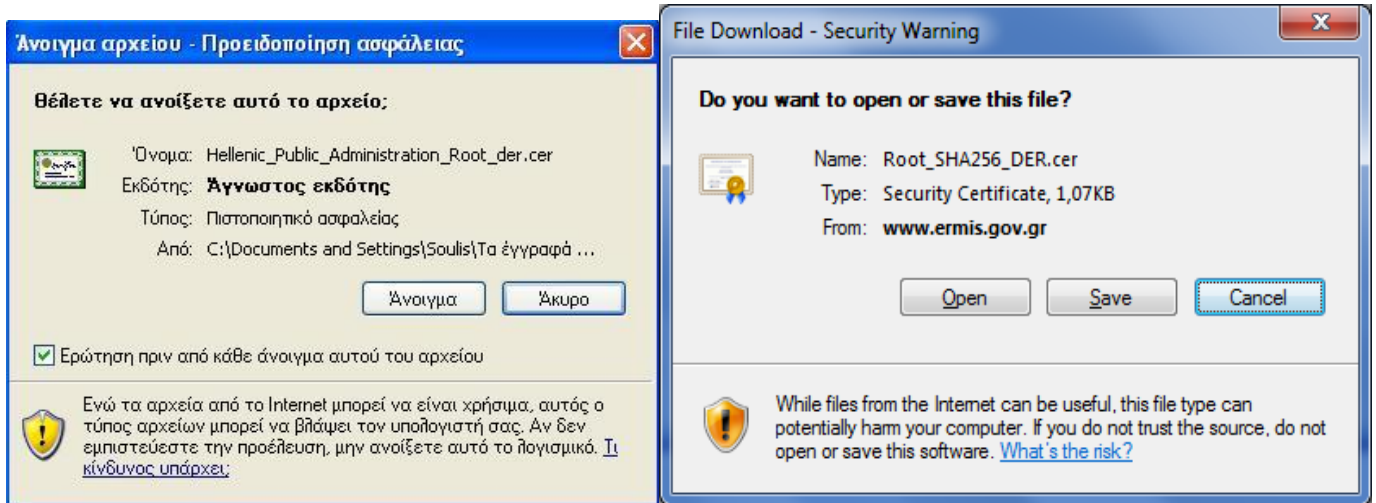


Εικόνα 1. Χώρος αποθήκευσης πιστοποιητικών Υποδομής Δημοσίου Κλειδιού της ΑΠΕΔ

2.1 Εγκατάσταση πιστοποιητικών Πρωτεύουσας Αρχής Πιστοποίησης

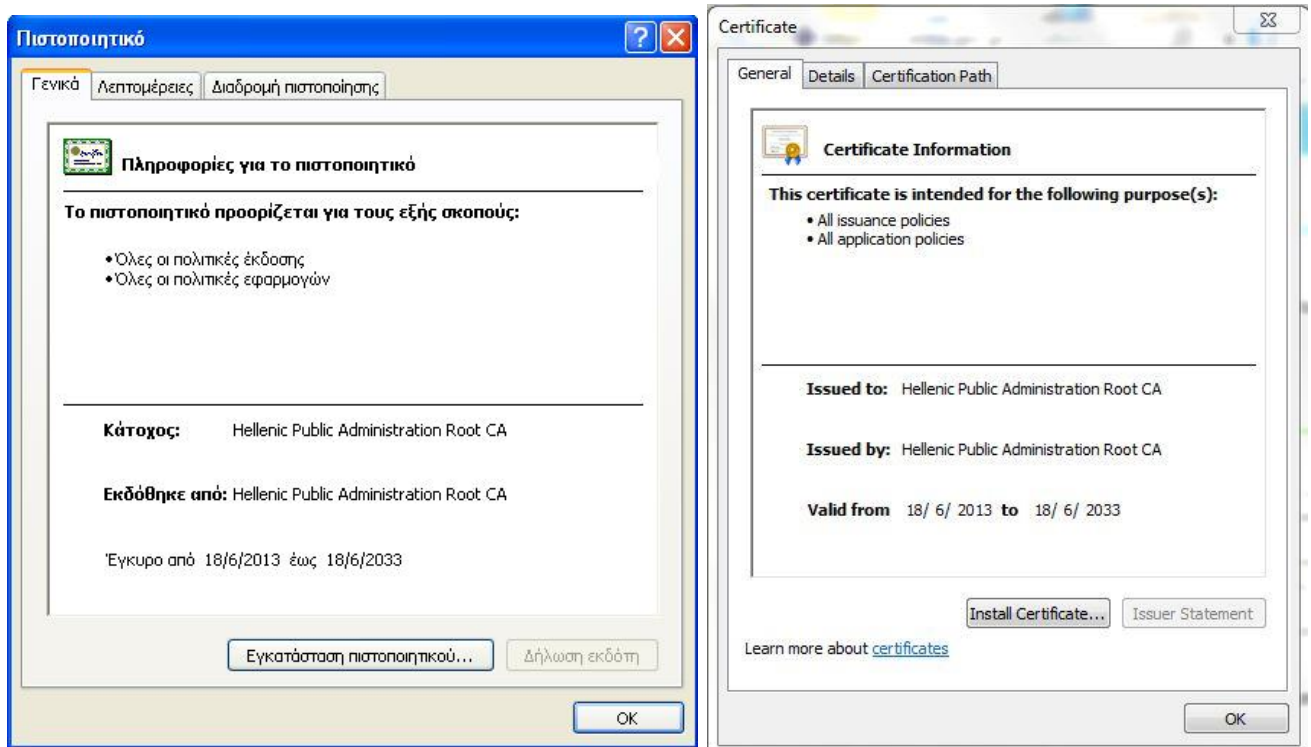
Σημείωση: Στις παρακάτω ενότητες παρουσιάζονται οθόνες τόσο για ελληνική (αριστερή εικόνα) όσο και για αγγλική έκδοση (δεξιά εικόνα) των Windows, για την καλύτερη κατανόηση και παρακολούθηση των απαραίτητων βημάτων.

1. Χρησιμοποιώντας τον Internet Explorer πηγαίνετε στο σύνδεσμο 1.1 **Πρωτεύουσας Αρχής Πιστοποίησης σε μορφή DER, Base64**, Εικόνα 1. Επιλέξτε **DER** (ή base64 σύμφωνα με τις ανάγκες της εφαρμογής – αν δεν υπάρχει κάποια ιδιαιτερότητα οι δύο επιλογές DER και base64 είναι ισοδύναμες) και στην συνέχεια εμφανίζεται η **Εικόνα 2** όπου και πρέπει να επιλέξετε **Άνοιγμα** (Open):



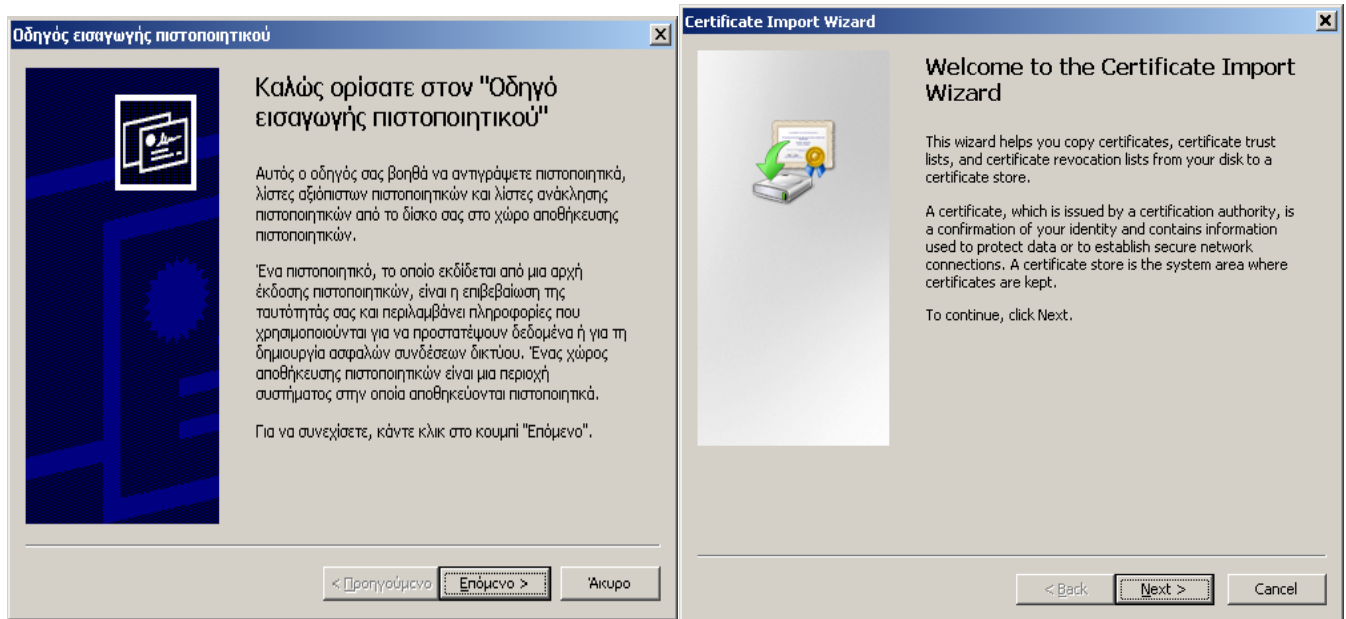
Εικόνα 2. Εγκατάσταση πιστοποιητικού ΠΑΠ της ΑΠΕΔ - Άνοιγμα

2. Στην Εικόνα 3 με τίτλο **Certificate** που εμφανίζεται, επιλέξτε **Εγκατάσταση Πιστοποιητικού** (Install Certificate).



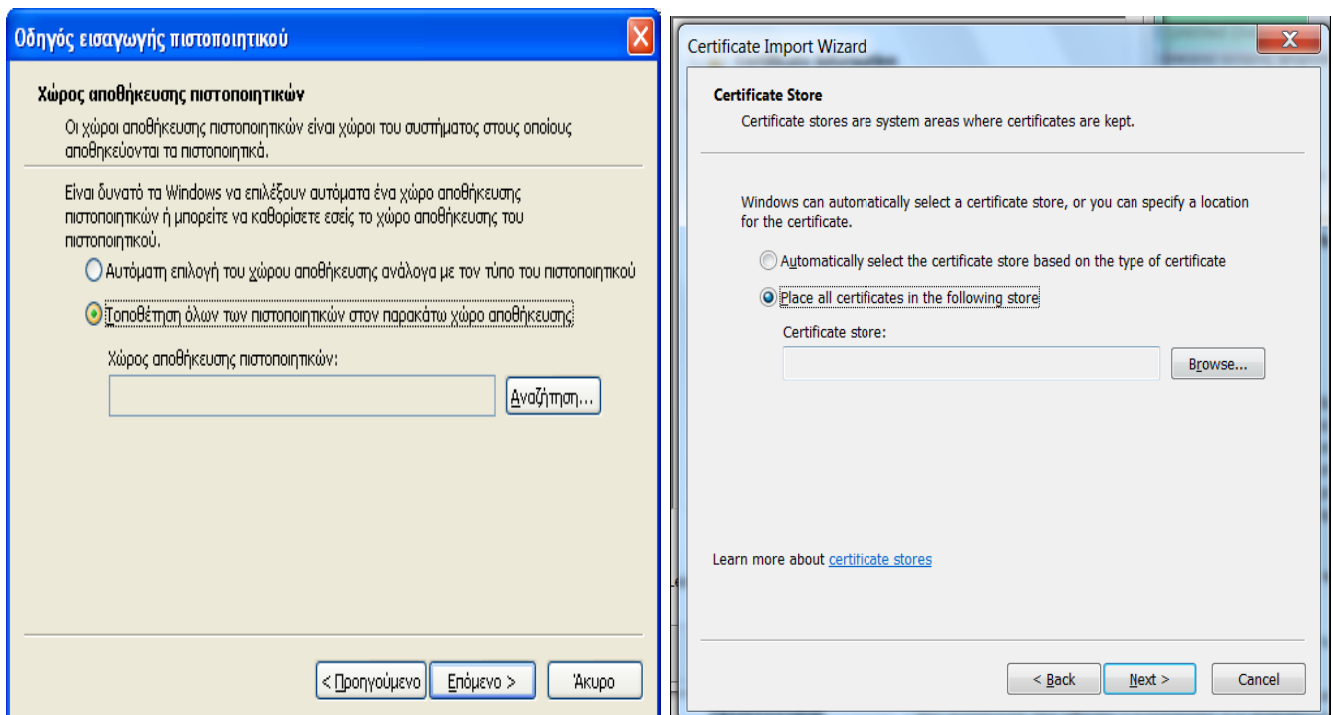
Εικόνα 3. Εγκατάσταση πιστοποιητικού ΠΑΠ της ΑΠΕΔ - Εγκατάσταση

3. Στο παράθυρο **Οδηγός εισαγωγής πιστοποιητικού** (Certificate Import Wizard) που εμφανίζεται στην **Εικόνα 4**, επιλέξτε **Επόμενο** (Next).



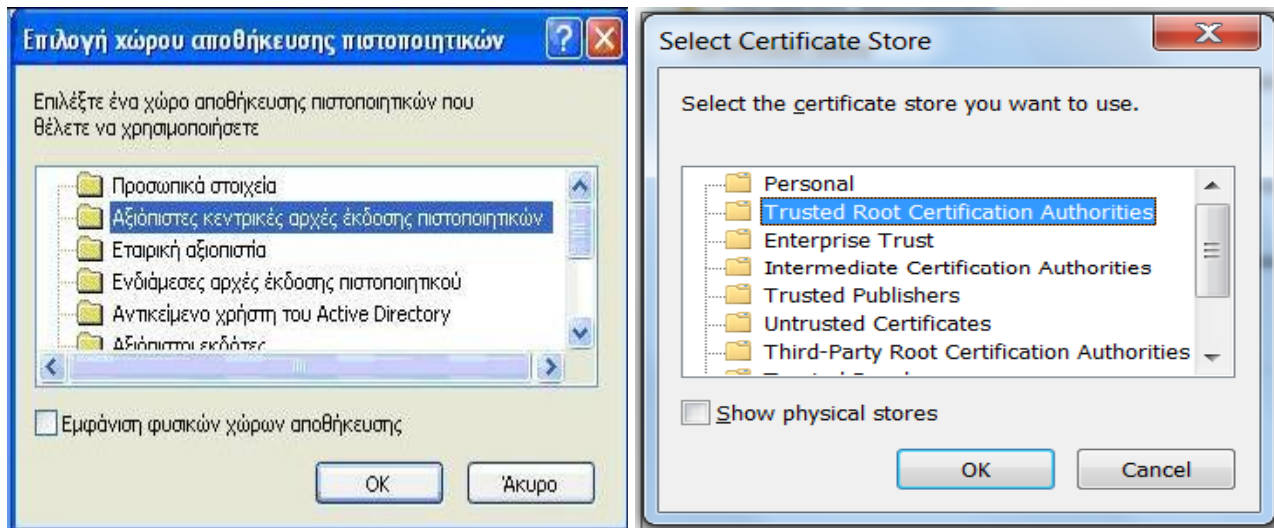
Εικόνα 4. Οδηγός εισαγωγής πιστοποιητικού ΠΑΠ της ΑΠΕΔ

4. Επιλέξτε **Τοποθέτηση όλων των πιστοποιητικών στον παρακάτω χώρο αποθήκευσης** (Place all certificates in the following store) και στην συνέχεια **Αναζήτηση** (browse) όπως φαίνεται στην **Εικόνα 5**.



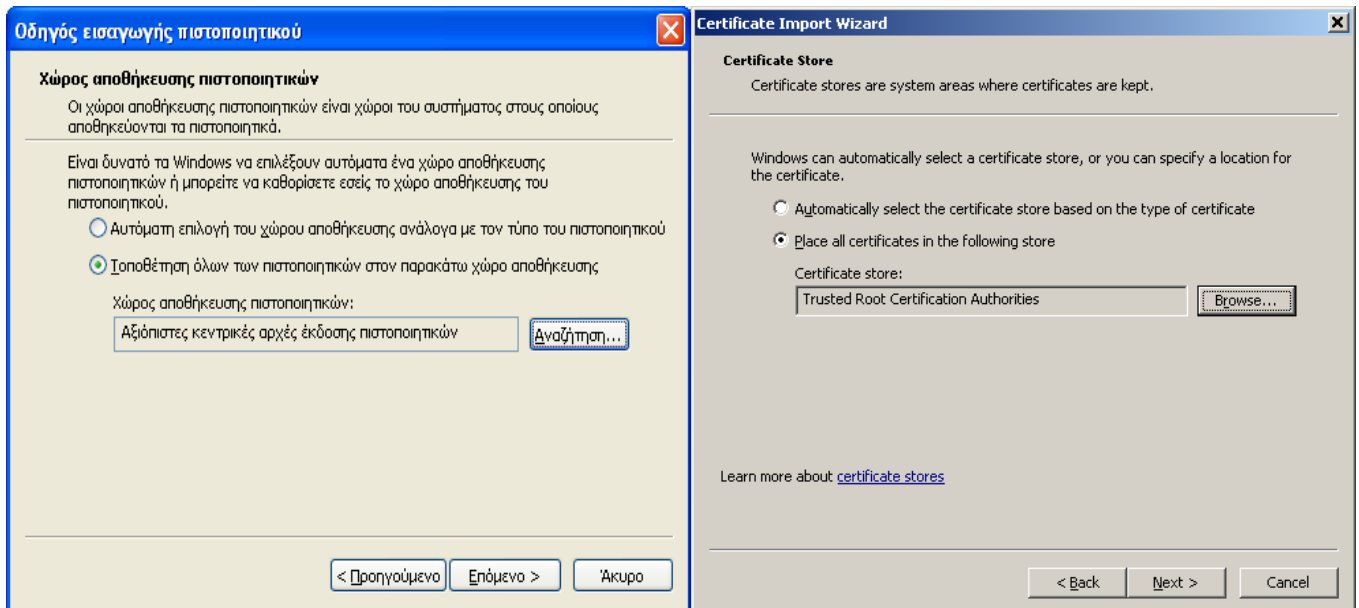
Εικόνα 5. Οδηγός εισαγωγής πιστοποιητικού ΠΑΠ της ΑΠΕΔ

5. Στην **Εικόνα 6** επιλέξτε **Αξιόπιστες κεντρικές αρχές έκδοσης πιστοποιητικών** (Trusted Root Certification Authorities).



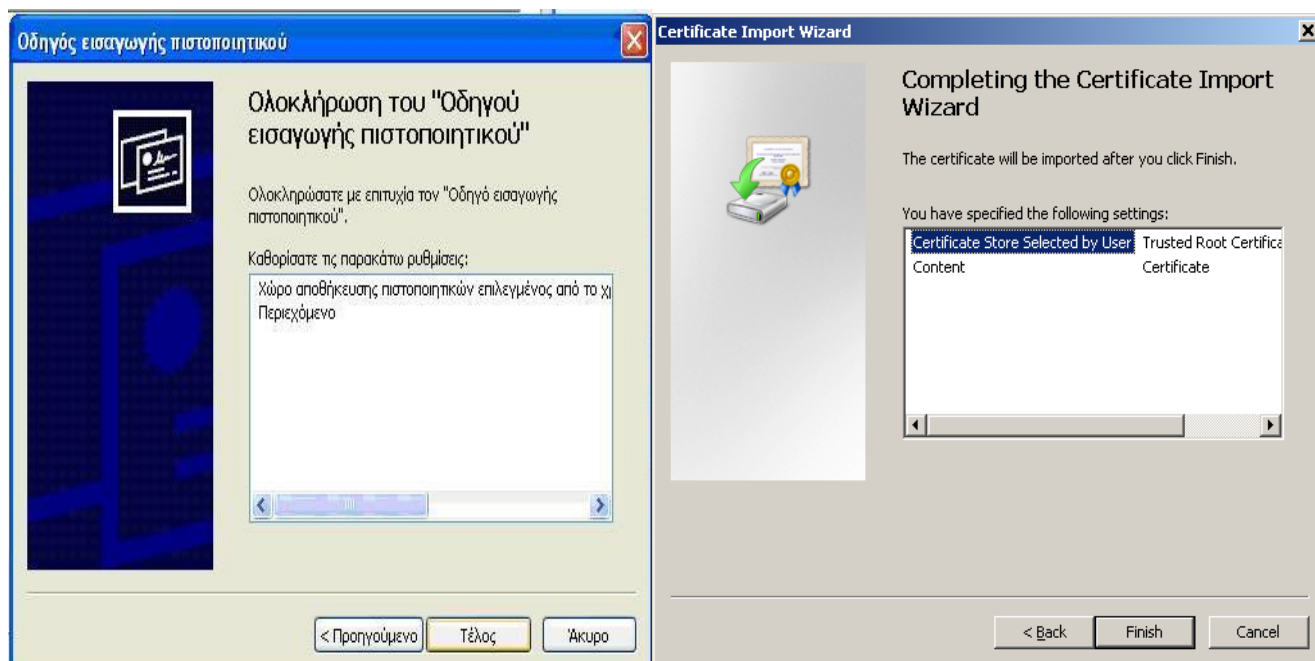
Εικόνα 6. Οδηγός εισαγωγής πιστοποιητικού ΠΑΠ της ΑΠΕΔ

Πατήστε **OK** στην **Εικόνα 6** και μας επιστρέφει το σύστημα στην **Εικόνα 7** όπου και πρέπει να πατήσετε **Επόμενο** (Next).



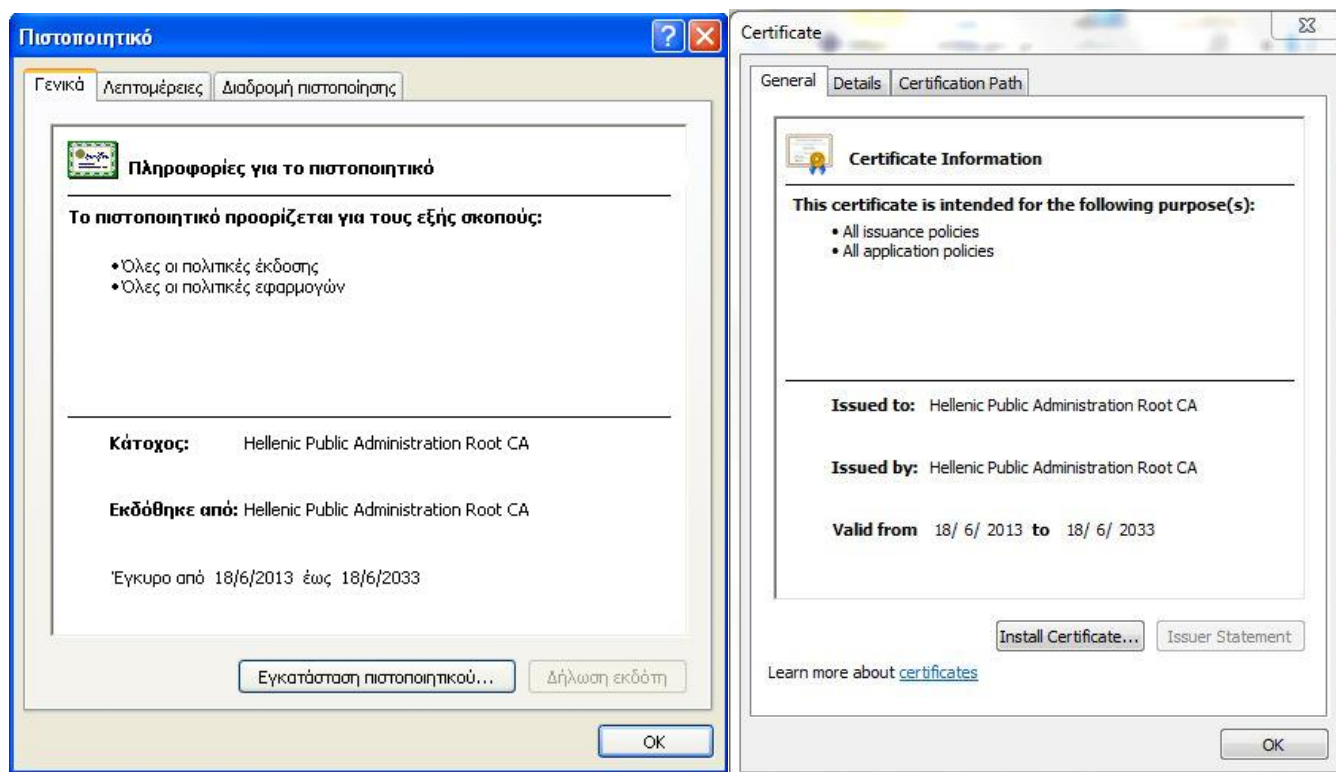
Εικόνα 7. Οδηγός εισαγωγής πιστοποιητικού ΠΑΠ της ΑΠΕΔ

Στην συνέχεια εμφανίζεται η **Εικόνα 8** που μας ενημερώνει ότι ολοκληρώθηκε ο οδηγός εισαγωγής του πιστοποιητικού.



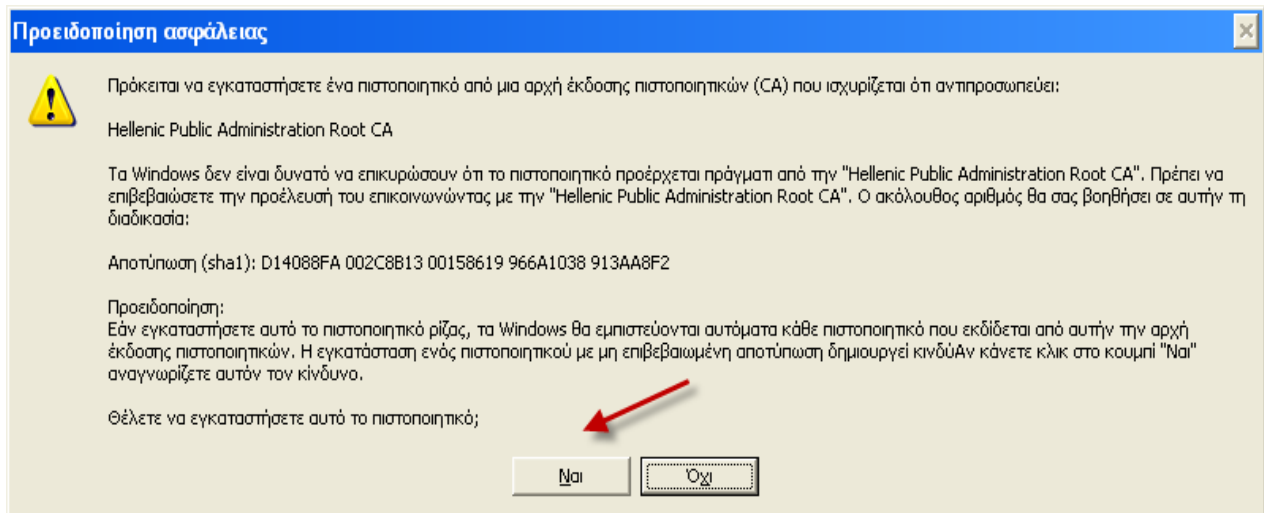
Εικόνα 8. Οδηγός εισαγωγής πιστοποιητικού ΠΑΠ της ΑΠΕΔ

Στην **Εικόνα 8** πατάμε **Τέλος** και στη συνέχεια πατήστε **OK** στην **Εικόνα 9**



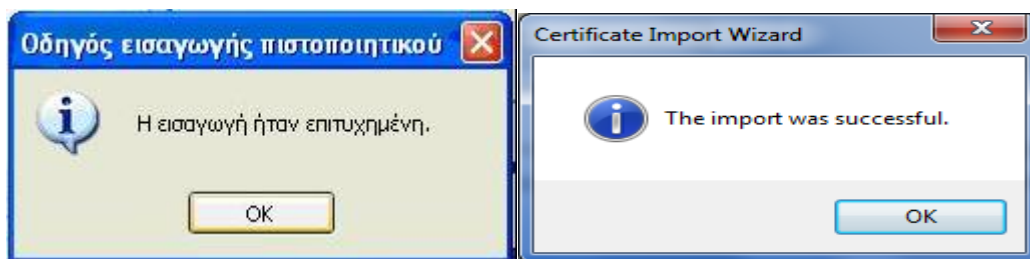
Εικόνα 9. Οδηγός εισαγωγής πιστοποιητικού ΠΑΠ της ΑΠΕΔ – Βήμα 6

Στην **Εικόνα 10** πατήστε **ΝΑΙ** (Yes).



Εικόνα 10. Οδηγός εισαγωγής πιστοποιητικού ΠΑΠ – Βήμα 7

Έχετε πλέον ολοκληρώσει με επιτυχία την εισαγωγή του πιστοποιητικού της ΠΑΠ (**Εικόνα 11**) – πατήστε **OK**.



Εικόνα 11. Οδηγός εισαγωγής πιστοποιητικού ΠΑΠ – Βήμα 8

Υπενθύμιση: Η παραπάνω διαδικασία περιγράφει την εγκατάσταση των πιστοποιητικών της ΠΑΠ της ΑΠΕΔ για πιστοποιητικά τα οποία εκδόθηκαν μετά από τη 01/08/2013. Επιπλέον θα πρέπει να επαναληφθεί η ίδια διαδικασία και για την εγκατάσταση πιστοποιητικών της ΠΑΠ της ΑΠΕΔ και για εκείνα που εκδόθηκαν πριν από τη 01/08/2013. Πιο συγκεκριμένα εγκαθιστούμε τα:

- **3.1 Πρωτεύουσας Αρχής Πιστοποίησης για πολίτες (SHA1) σε μορφή DER ή Base64 ,**
- **3.3 Πρωτεύουσας Αρχής Πιστοποίησης για πολίτες (SHA2) σε μορφή DER ή Base64 και**

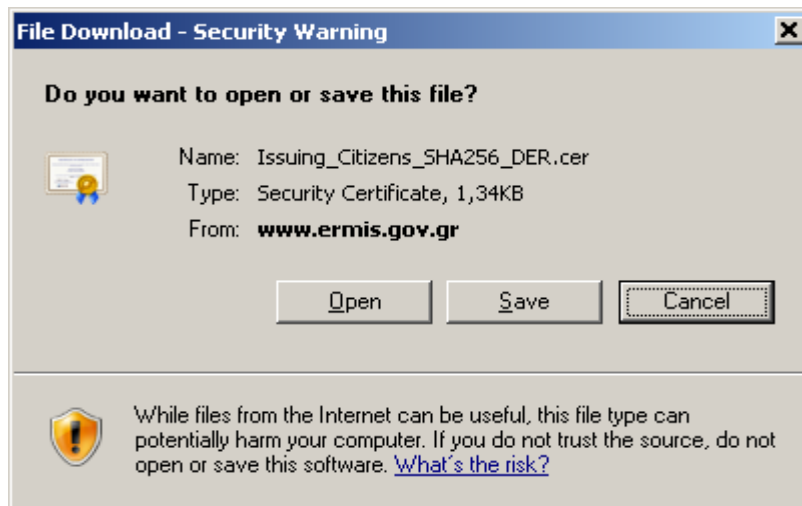
(Εικόνα 1) με τον ίδιο ακριβώς τρόπο που περιεγράφηκε παραπάνω. Τα παραπάνω Τα πιστοποιητικά είναι διαθέσιμα στον χώρο αποθήκευσης Υποδομής Δημοσίου Κλειδιού ΕΡΜΗΣ που βρίσκονται στην σελίδα <https://pki.ermis.gov.gr/repository.html>

Στην περίπτωση που χρειάζεται να γίνει χρήση των πιστοποιητικών με Mozilla Thunderbird, συστήνεται να επαναληφθεί η παραπάνω διαδικασία με φυλλομετρητή Mozilla Firefox.

2.2 Εγκατάσταση πιστοποιητικών της Υποκείμενης Αρχής Πιστοποίησης στον Internet Explorer

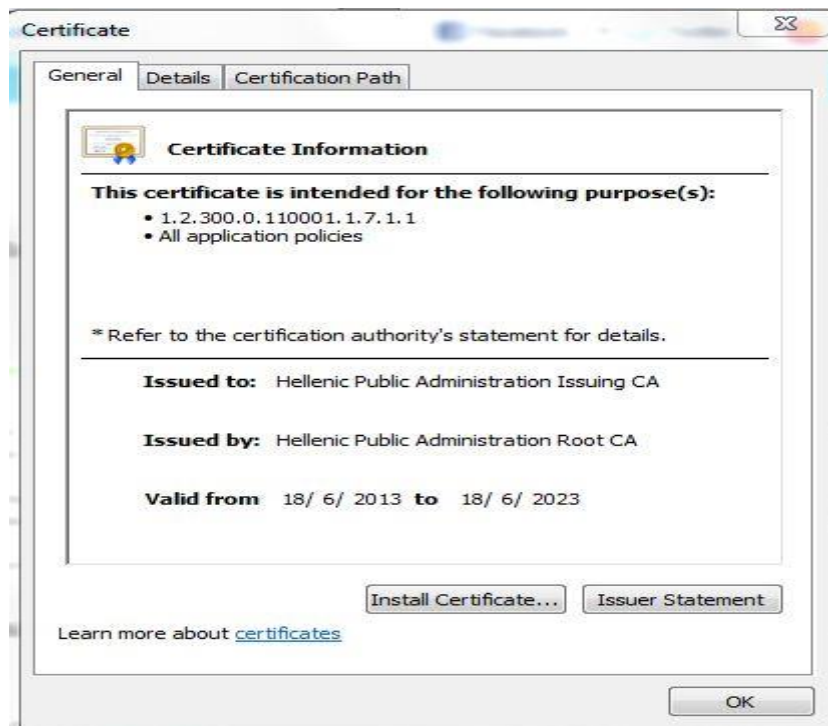
Τα πιστοποιητικά είναι διαθέσιμα στον χώρο αποθήκευσης Υποδομής Δημοσίου Κλειδιού ΕΡΜΗΣ που βρίσκονται στην σελίδα <https://pki.ermis.gov.gr/repository.html>, όπως φαίνεται στην Εικόνα 1.

1. Χρησιμοποιώντας τον Internet Explorer πηγαίνετε στο σύνδεσμο **1.2 Υποκείμενης Αρχής Πιστοποίησης σε μορφή DER ή Base64**, Εικόνα 12. Επιλέξτε **DER** και στην συνέχεια εμφανίζεται το παρακάτω παράθυρο (Εικόνα 12) όπου και πρέπει να επιλέξετε **Άνοιγμα** (Open):



Εικόνα 12. Εγκατάσταση πιστοποιητικού ΥπΑΠ της ΑΠΕΔ

2. Στην Εικόνα 13 με τίτλο **Certificate** επιλέξτε **Εγκατάσταση Πιστοποιητικού** (Install Certificate).



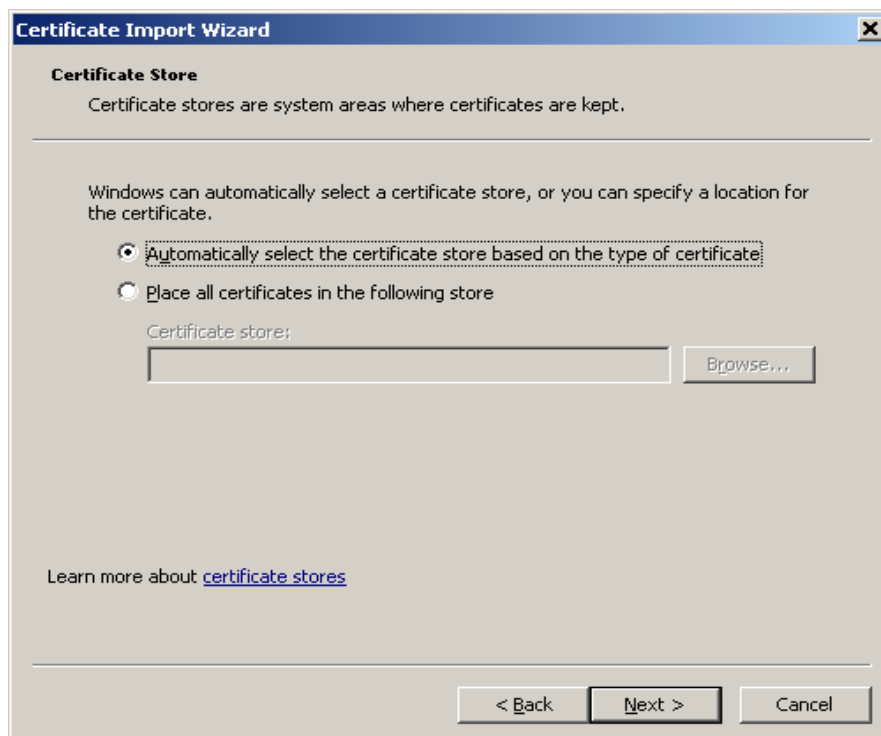
Εικόνα 13. Εγκατάσταση πιστοποιητικού ΥπΑΠ της ΑΠΕΔ – Βήμα 2

3. Στο παράθυρο **Οδηγός εισαγωγής πιστοποιητικού** (Certificate Import Wizard) που εμφανίζεται στην **Εικόνα 14**, επιλέξτε **Επόμενο** (Next).



Εικόνα 14. Οδηγός εισαγωγής πιστοποιητικού ΥπΑΠ της ΑΠΕΔ – Βήμα 1

4. Επιλέξτε **Αυτόματη επιλογή του χώρου αποθήκευσης σύμφωνα με τον τύπο του πιστοποιητικού** (Automatically select the certificate store based on the type of certificate), όπως φαίνεται στην **Εικόνα 15**.



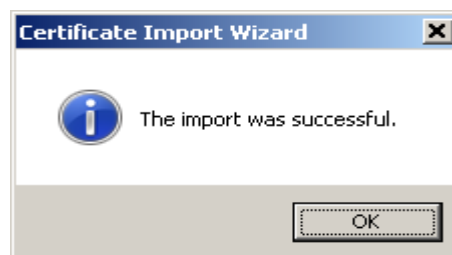
Εικόνα 15. Οδηγός εισαγωγής πιστοποιητικού ΥπΑΠ της ΑΠΕΔ – Βήμα 2

Στην **Εικόνα 16** επιλέγετε **Ναι** (Yes).



Εικόνα 16. Οδηγός εισαγωγής πιστοποιητικού ΥπΑΠ της ΑΠΕΔ – Βήμα 4

Έχετε πλέον ολοκληρώσει με επιτυχία (Εικόνα 17) την εισαγωγή του πιστοποιητικού της Υποκείμενης Αρχής Πιστοποίησης της ΑΠΕΔ.



Εικόνα 17. Ολοκλήρωση οδηγού εισαγωγής πιστοποιητικού ΥπΑΠ της ΑΠΕΔ – Βήμα 5

Υπενθύμιση: Η παραπάνω διαδικασία περιγράφει την εγκατάσταση των πιστοποιητικών της ΥπΑΠ της ΑΠΕΔ για όσα πιστοποιητικά εκδόθηκαν μετά τη 01/08/2013. Θα πρέπει να επαναληφθεί ως έχει και για την εγκατάσταση των πιστοποιητικών της Υποκείμενης Αρχής Πιστοποίησης της ΑΠΕΔ και για εκείνα που εκδόθηκαν πριν από 01/08/2013. Πιο συγκεκριμένα εγκαθιστούμε τα:

- **3.2 Υποκείμενης Αρχής Πιστοποίησης για πολίτες (SHA1) σε μορφή DER ή Base64 ,**
- **3.4 Υποκείμενης Αρχής Πιστοποίησης για πολίτες (SHA2) σε μορφή DER ή Base64**

(Εικόνα 1) με τον ίδιο ακριβώς τρόπο που περιεγράφηκε παραπάνω. Τα παραπάνω Τα πιστοποιητικά είναι διαθέσιμα στον χώρο αποθήκευσης Υποδομής Δημοσίου Κλειδιού ΕΡΜΗΣ που βρίσκονται στην σελίδα <https://pki.ermis.gov.gr/repository.html>

Στην περίπτωση που χρειάζεται να γίνει χρήση των πιστοποιητικών με Mozilla Thunderbird, συστήνεται να επαναληφθεί η παραπάνω διαδικασία με φυλλομετρητή Mozilla Firefox.

3. Εγκατάσταση πιστοποιητικών χρονοσήμανσης (TSA) της ΑΠΕΔ

Προκειμένου τα έγγραφα να διαθέτουν ασφαλή χρονοσήμανση (ήτοι ημερομηνία και ώρα από πιστοποιημένο πάροχο υπηρεσίας χρονοσήμανσης και όχι από το ρολόι του υπολογιστή) θα πρέπει να εγκατασταθούν τα αντίστοιχα πιστοποιητικά χρονοσήμανσης της ΑΠΕΔ. Στην ενότητα 5 της ιστοσελίδας <https://pki.ermis.gov.gr/repository.html> βρίσκονται όλα τα πιστοποιητικά ασφαλούς χρονοσήμανσης, όπως φαίνεται και στη παρακάτω εικόνα.

5. Πιστοποιητικά χρονοσήμανσης Αρχής Πιστοποίησης Ελληνικού Δημοσίου

5.1 Αρχής Χρονοσήμανσης #1 σε μορφή DER, Base64

- Από 1/8/2013 και έπειτα
- Thumbprint Algorithm: SHA2
- Thumbprint: d8 ba 52 c8 e4 9b 22 7f 03 79 0b 55 ec 80 e5 d4 93 b0 bb 0a

5.3 Αρχής Χρονοσήμανσης Α σε μορφή DER, Base64

- Πριν από 1/8/2013
- Thumbprint Algorithm: SHA2
- Thumbprint: 67 88 a7 7c 0e c4 6c 4e 39 3e 39 bb 05 4b c0 90 f2 8c bd b1

5.5 Πιστοποιητικό Υποκείμενης Αρχής Χρονοσήμανσης σε μορφή DER

- Μετά από 1/8/2013
- Thumbprint Algorithm: SHA2
- Thumbprint: 59 f0 15 10 cf 95 41 7d dd 2e ee 9e c1 9a 89 c2 27 1a f6 ca
- Subject key identifier: 56 e0 ae b4 aa 0e 82 f3 8b 33 83 de 3f 4e c8 e6 a1 38 75 04

5.2 Αρχής Χρονοσήμανσης #2 σε μορφή DER, Base64

- Από 1/8/2013 και έπειτα
- Thumbprint Algorithm: SHA2
- Thumbprint: c6 47 20 f3 d5 4b 5b 31 5b 56 49 c6 03 13 d6 0f 95 f3 36 42

5.4 Αρχής Χρονοσήμανσης Β σε μορφή DER, Base64

- Πριν από 1/8/2013
- Thumbprint Algorithm: SHA2
- Thumbprint: e4 85 d3 b4 ff 99 13 4a f0 3a f5 18 44 22 18 81 ba 59 a4 9b

5.6 Πιστοποιητικό Υποκείμενης Αρχής Χρονοσήμανσης σε μορφή Base64

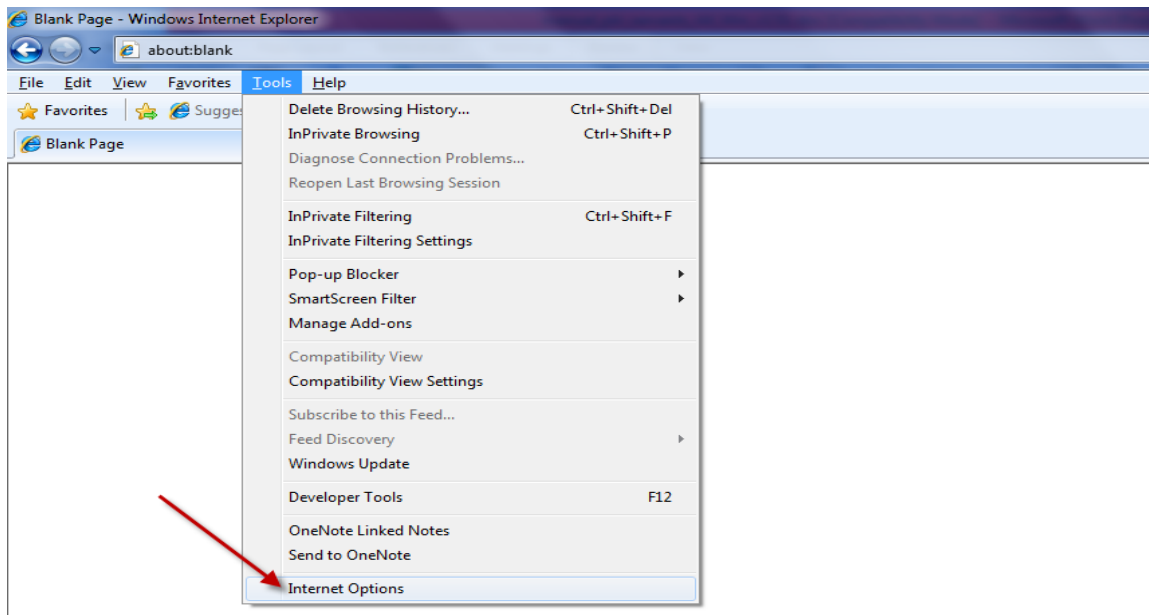
- Μετά από 1/8/2013
- Thumbprint Algorithm: SHA2
- Thumbprint: 59 f0 15 10 cf 95 41 7d dd 2e ee 9e c1 9a 89 c2 27 1a f6 ca
- Subject key identifier: 56 e0 ae b4 aa 0e 82 f3 8b 33 83 de 3f 4e c8 e6 a1 38 75 04

Εικόνα 18 Πιστοποιητικά χρονοσήμανσης της ΑΠΕΔ

Όπως φαίνεται και από την Εικόνα 18, εγκαθιστούμε τα πιστοποιητικά της ενότητας 5.3 και 5.4 με τον ίδιο ακριβώς τρόπο όπως και τα Πιστοποιητικά της Πρωτεύουσας Αρχής Πιστοποίησης (σελίδα 4). Δηλαδή όλα τα πιστοποιητικά θα πρέπει να αποθηκευτούν στις αξιόπιστες κεντρικές αρχές έκδοσης πιστοποιητικών. Εγκαθιστούμε τα πιστοποιητικά 5.1, 5.2, 5.5 και 5.6 με τον ίδιο ακριβώς τρόπο όπως και τα Πιστοποιητικά της Υποκείμενης Αρχής Πιστοποίησης (σελίδα 10).

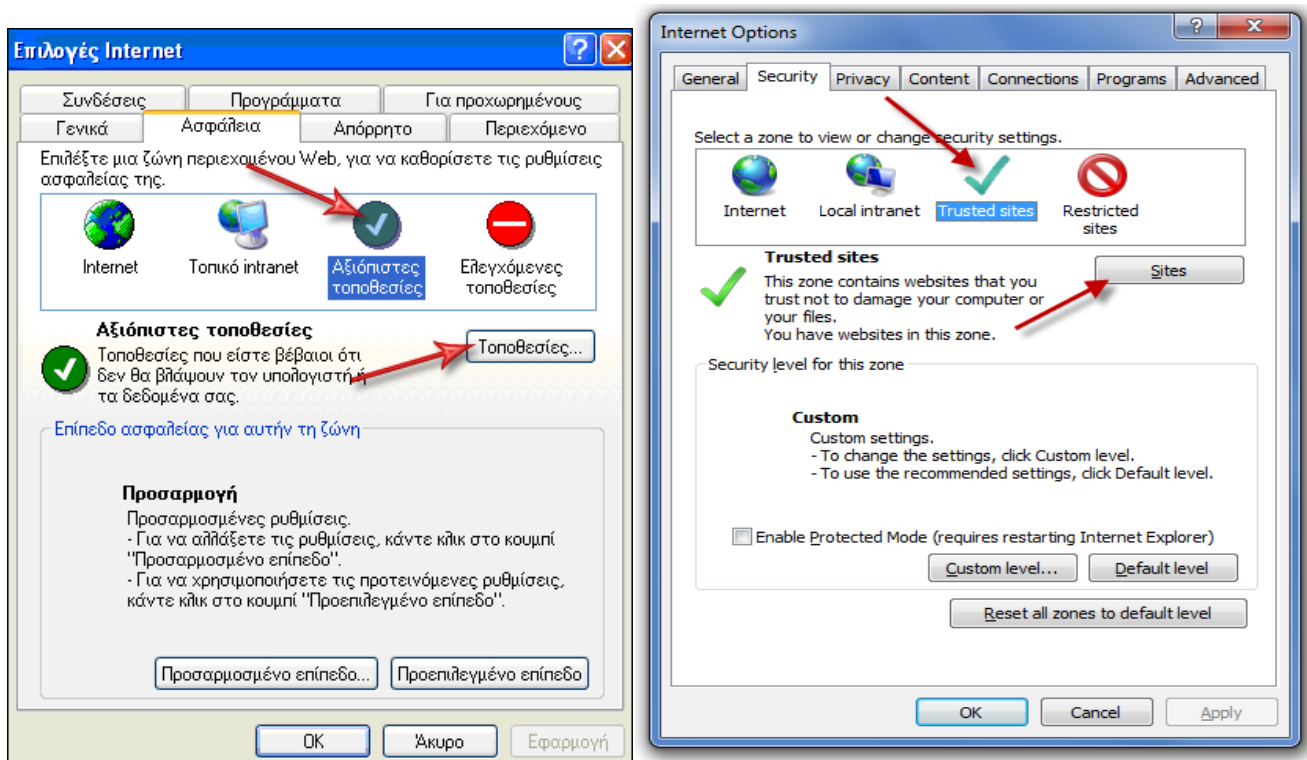
4. Προετοιμασία φυλλομετρητή (web browser)

Αφού εγκατασταθούν στον Internet Explorer τα πιστοποιητικά της ΑΠΕΔ, απαιτείται να εκτελεστούν τα ακόλουθα βήματα. Στο μενού εργαλείων του Internet Explorer (Εικόνα 19), επιλέξτε **Εργαλεία (tools)** και έπειτα **Επιλογές Internet** (Internet Options).



Εικόνα 19. Internet Explorer – Εργαλεία – Επιλογές Internet (Tools – Internet Options)

2. Στο παράθυρο που εμφανίζεται, επιλέξτε την καρτέλα **Ασφάλεια** (Security). Από την καρτέλα **Ασφάλεια**, επιλέξτε **Αξιόπιστες τοποθεσίες** (trusted sites) και έπειτα **Τοποθεσίες** (sites) (Εικόνα 20).



Εικόνα 20. Internet Explorer – Επιλογές Internet – Ασφάλεια – Αξιόπιστες τοποθεσίες (Security – Trusted Sites)

3. Προσθέστε τις δύο παρακάτω τοποθεσίες στη λίστα αξιόπιστων τοποθεσιών, πληκτρολογώντας τις στο πλαίσιο και επιλέγοντας **Προσθήκη** όπως φαίνεται στην Εικόνα 21.

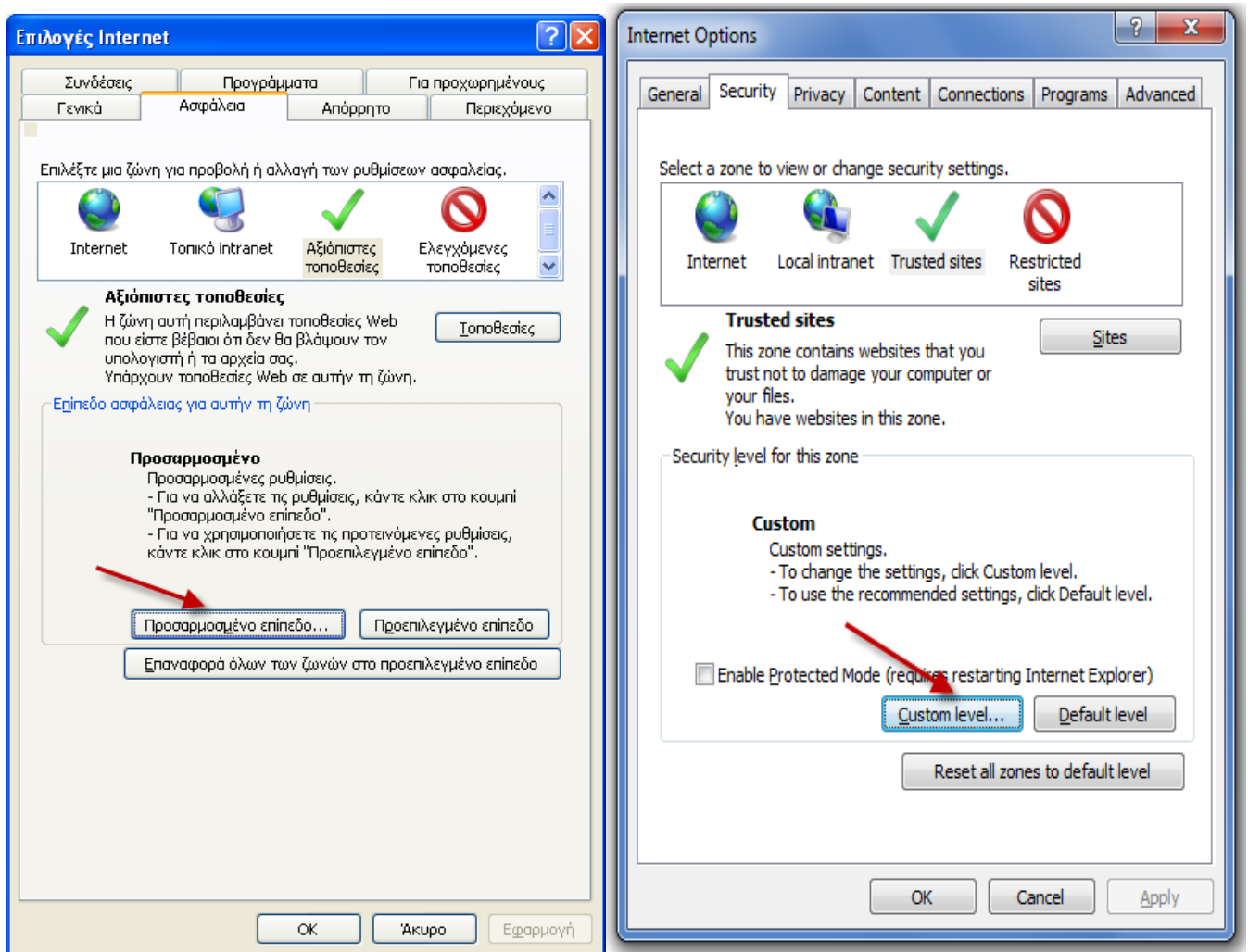
<https://mpki.ermis.gov.gr>

<https://pki.ermis.gov.gr>



Εικόνα 21. Προσθήκη αξιόπιστων τοποθεσιών στον Internet Explorer

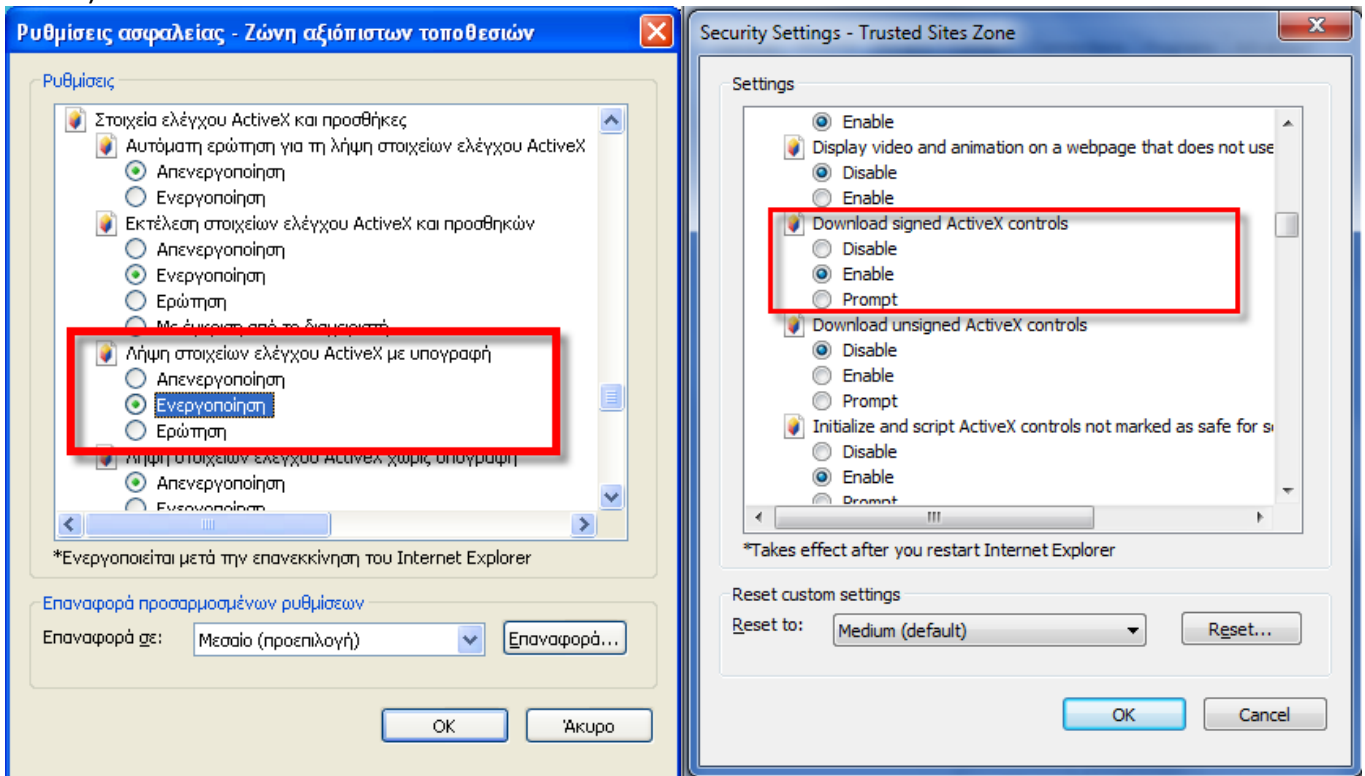
4. Παραμένοντας στην καρτέλα Ασφάλεια (Security) και έχοντας επιλέξει τις **Αξιόπιστες Τοποθεσίες** Εικόνα 22 επιλέγετε **Προσαρμοσμένο Επίπεδο** ("Custom Level") και ενεργοποιείτε τα παρακάτω:



Εικόνα 22. Προσαρμοσμένες ρυθμίσεις ασφάλειας Internet Explorer

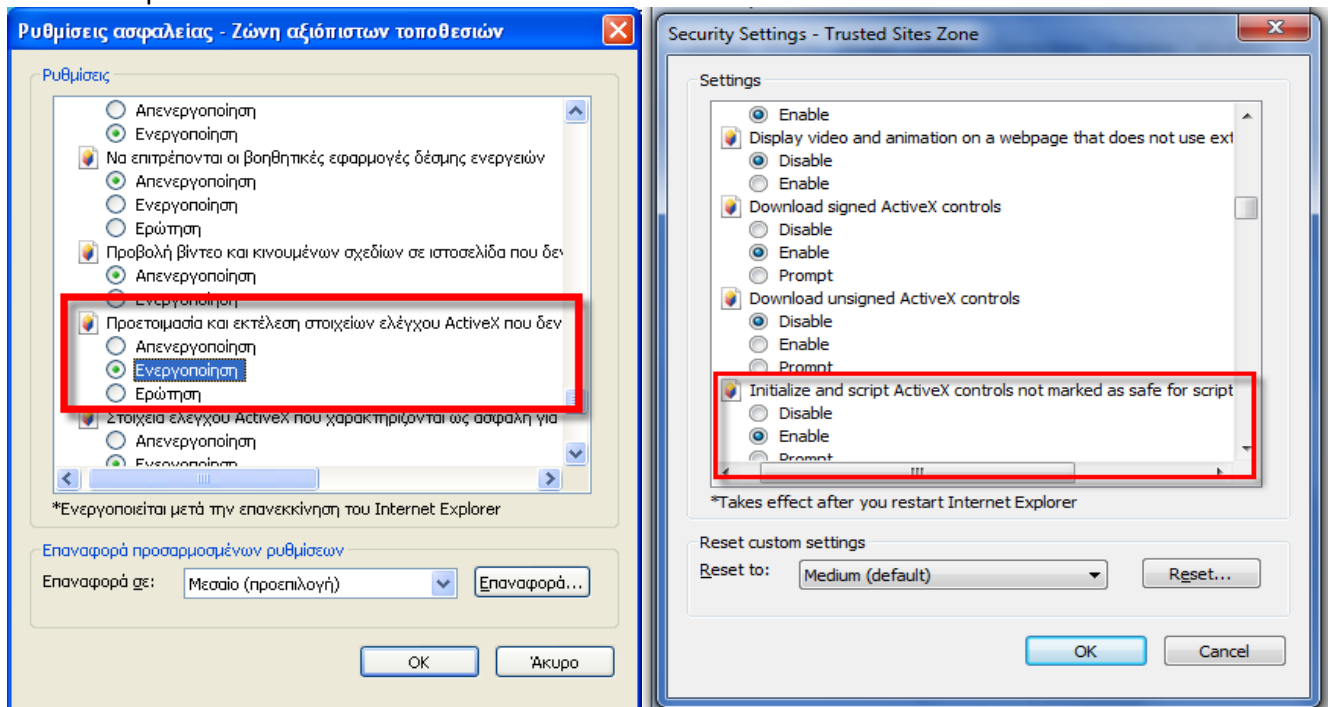
Σε συνέχεια θα πρέπει να ενεργοποιήσετε τα στοιχεία ελέγχου ActiveX που περιγράφονται πιο κάτω:

1) Λήψη στοιχείων ελέγχου ActiveX με υπογραφή – Ενεργοποίηση (Download signed ActiveX controls = Enable) - **Εικόνα 23**



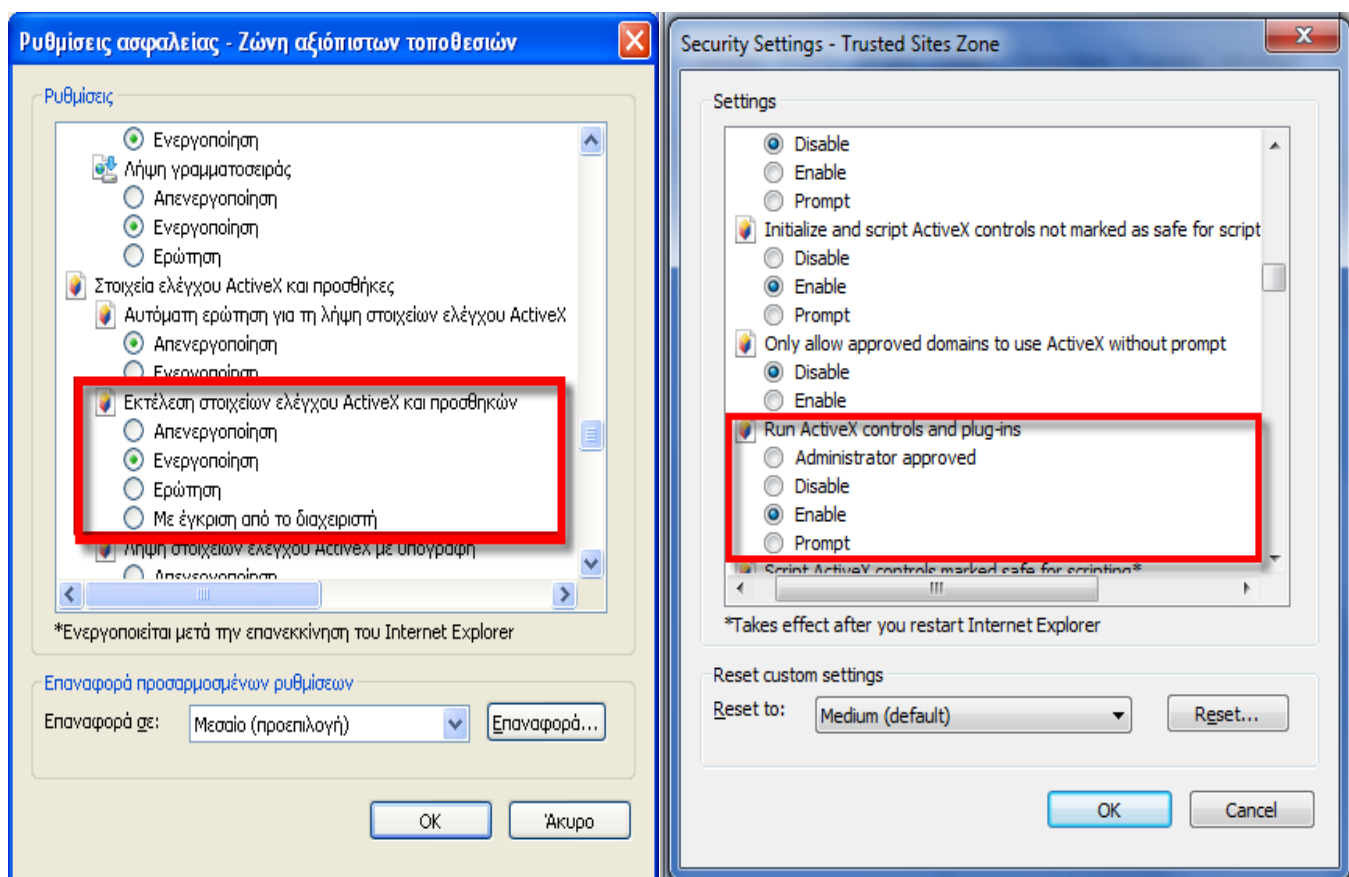
Εικόνα 23. Προσαρμοσμένες ρυθμίσεις ασφάλειας Internet Explorer – Ενεργοποίηση λήψης στοιχείων ελέγχου ActiveX με υπογραφή

2) Προετοιμασία και εκτέλεση στοιχείων ελέγχου ActiveX που δεν χαρακτηρίζονται ως ασφαλή – Ενεργοποίηση (Initialize and script ActiveX controls not marked as safe for scripting – Enable), όπως φαίνεται στην **Εικόνα 24**



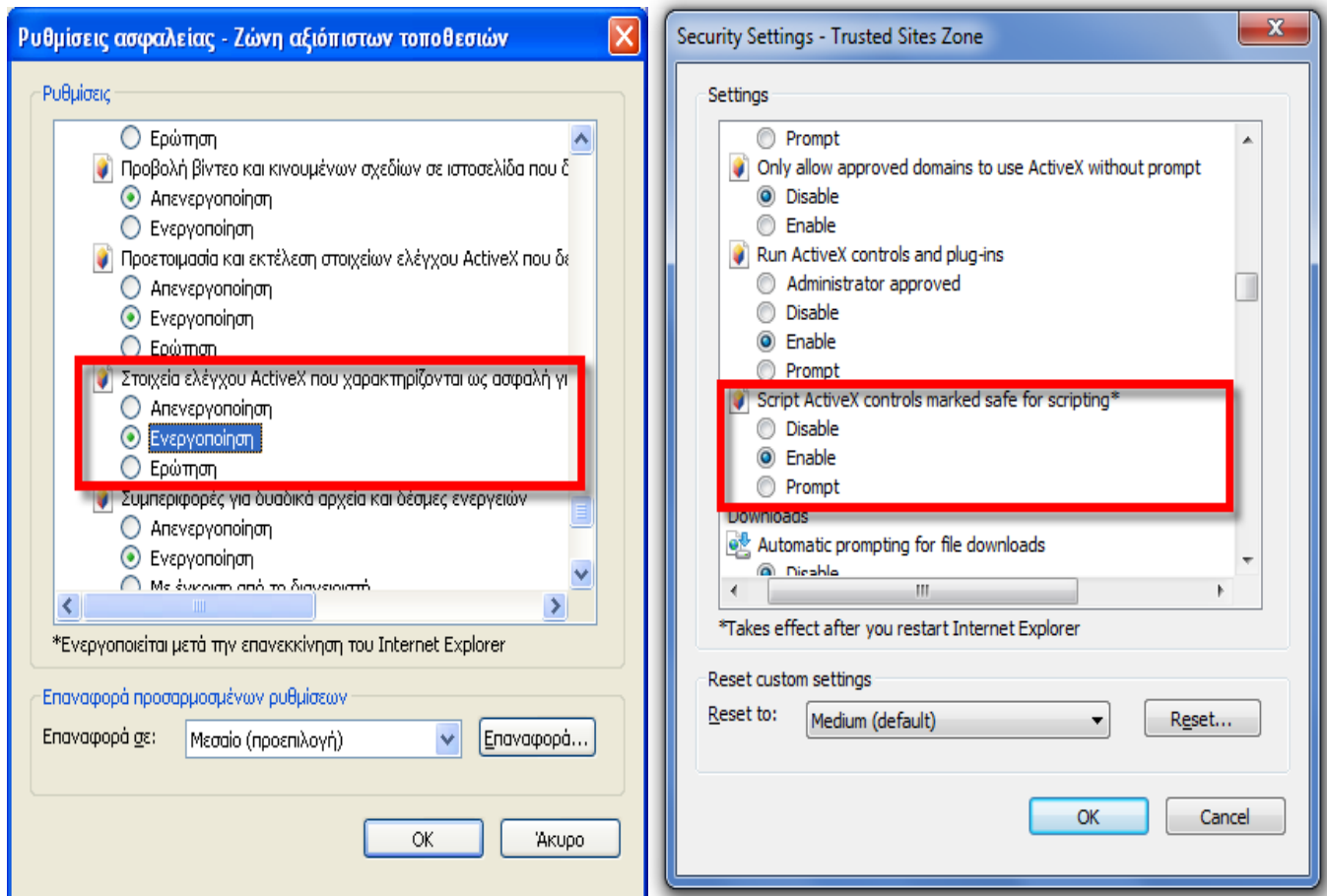
Εικόνα 24. Προσαρμοσμένες ρυθμίσεις ασφάλειας Internet Explorer – Ενεργοποίηση προετοιμασίας και εκτέλεσης στοιχείων ελέγχου ActiveX που δεν χαρακτηρίζονται ως ασφαλή

3) Εκτέλεση στοιχείων ελέγχου ActiveX και προσθηκών – Ενεργοποίηση (Run ActiveX controls and Plugins = Enable) - **Εικόνα 25**



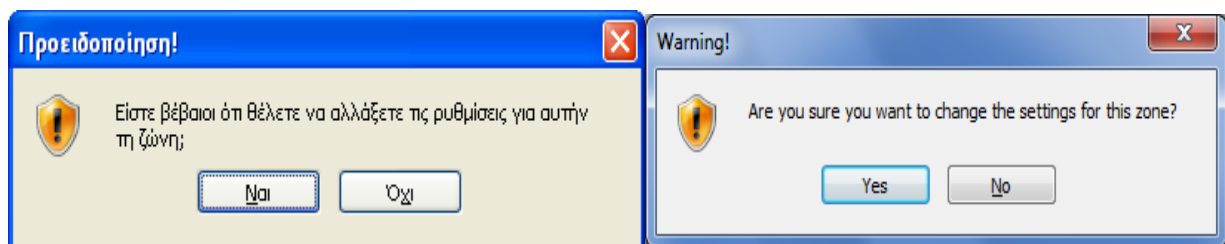
Εικόνα 25. Εκτέλεση στοιχείων ελέγχου ActiveX και προσθηκών

4) Στοιχεία ελέγχου ActiveX που χαρακτηρίζονται ως ασφαλή για εκτέλεση – Ενεργοποίηση (Script ActiveX controls marked safe for scripting* = Enable) - Εικόνα 26.



Εικόνα 26. Στοιχεία ελέγχου ActiveX που χαρακτηρίζονται ως ασφαλή για εκτέλεση

Αφού ολοκληρώσουμε τις παραπάνω αλλαγές επιλέγουμε **OK** και εμφανίζεται η **Εικόνα 27** όπου επιλέγουμε **ΝΑΙ** για επιβεβαίωση των αλλαγών.



Εικόνα 27. Προσαρμοσμένες ρυθμίσεις ασφάλειας Internet Explorer – Επιβεβαίωση αλλαγής ρυθμίσεων

5. Τέλος, κλείστε όλα τα ανοιχτά παράθυρα του Internet Explorer και επανεκκινήστε τον Internet Explorer.