ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΪΑΤΡΙΚΗ

ΗΛΕΚΤΡΟΝΙΚΗ ΑΝΤΑΛΛΑΓΗ ΕΓΓΡΑΦΩΝ ΚΑΙ ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ

ΚΑΠΕΡΩΝΗ ΒΑΡΒΑΡΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

Αθανάσιος Λουκόπουλος

Λαμία, Ιούλιος 2019

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

ELECTRONIC DOCUMENT EXCHANGE AND DIGITAL SIGNATURE IN THE PUBLIC SECTOR

KAPERONI VARVARA

MASTER THESIS

Supervisor

Athanasios Loukopoulos

Lamia, July 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΪΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

ΗΛΕΚΤΡΟΝΙΚΗ ΑΝΤΑΛΛΑΓΗ ΕΓΓΡΑΦΩΝ ΚΑΙ ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ

ΚΑΠΕΡΩΝΗ ΒΑΡΒΑΡΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

Αθανάσιος Λουκόπουλος

Λαμία, Ιούλιος 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «Ηλεκτρονική ανταλλαγή εγγράφων και ψηφιακή υπογραφή στον Δημόσιο Τομέα» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Η ΔΗΛΟΥΣΑ

10-07-2019

Υπογραφή

ΗΛΕΚΤΡΟΝΙΚΗ ΑΝΤΑΛΛΑΓΗ ΕΓΓΡΑΦΩΝ ΚΑΙ ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ

ΚΑΠΕΡΩΝΗ ΒΑΡΒΑΡΑ

Τριμελής Επιτροπή:

Δρ. Αθανάσιος Λουκόπουλος (επιβλέπων)

Δρ. Ιωάννης Αναγνωστόπουλος

Δρ. Γεώργιος Σταμούλης

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εκπονήθηκε με σκοπό να παρουσιάσει και να αναλύσει ένα σύγχρονο θέμα που αφορά την διευκόλυνση των πολιτών ως προς τις συναλλαγές τους με τον κρατικό μηχανισμό, **την ηλεκτρονική ανταλλαγή εγγράφων και την ψηφιακή υπογραφή στον Δημόσιο τομέα**.

Στο πρώτο κεφάλαιο εισάγονται οι ορισμοί της Ηλεκτρονικής Διακυβέρνησης και των Τεχνολογιών της Πληροφορίας και της Επικοινωνίας (ΤΠΕ) στην Ελλάδα, και αναλύονται οι βασικές αρχές αλλά και οι στόχοι της στρατηγικής του σχεδίου της Ηλεκτρονικής Διακυβέρνησης 2014-2020.

Στο δεύτερο κεφάλαιο γίνεται αναφορά στον ορισμό του ηλεκτρονικού εγγράφου, τον ορισμό της ηλεκτρονικής υπογραφής και τις μεθόδους κρυπτογράφησής της. Στη συνέχεια, αναλύονται τα στάδια δημιουργίας ψηφιακής υπογραφής και παρατίθενται πληροφορίες σχετικά με το πιστοποιητικό δημόσιου κλειδιού πιστοποιητικό δημόσιου κλειδιού, την Υποδομή Δημοσίου Κλειδιού (ΥΔΚ) και τις κατηγορίες Ασφαλών Διατάξεων Δημιουργίας Υπογραφής (ΑΔΔΥ).

Στο τρίτο κεφάλαιο, περιγράφεται αναλυτικά η διαδικασία έκδοσης ψηφιακής υπογραφής μέσω της Υποδομή Δημοσίου Κλειδιού (ΥΔΚ) της HARICA. Επίσης, περιγράφεται η διαδικασία ψηφιακής υπογραφής ενός αρχείου και ενός μηνύματος ηλεκτρονικού ταχυδρομείου.

Στο τέταρτο κεφάλαιο παρουσιάζεται συνοπτικά η διαδικασία έκδοσης ηλεκτρονικής υπογραφής μέσω της πύλης ΕΡΜΗΣ.

Στο πέμπτο κεφάλαιο αναλύεται το μέλλον των Πληροφοριακών Συστημάτων, το Μητρώο Πολιτών και η Κάρτα Πολίτη με σκοπό την ευέλικτη και αποτελεσματική δημόσια διοίκηση.

Τέλος, στο έκτο κεφάλαιο παρουσιάζεται το πολλά υποσχόμενο έργο του Κεντρικού Συστήματος Ηλεκτρονικής Διακίνησης Εγγράφων (ΣΗΔΕ), τα πλεονεκτήματά του και τα βασικά στοιχεία της αρχιτεκτονικής του.

ΛΕΞΕΙΣ-ΚΛΕΙΔΙΑ: Ψηφιακή Υπογραφή, Προσωπικό Ψηφιακό Πιστοποιητικό, Υποδομή Δημοσίου Κλειδιού, Ασφαλής Διάταξη Δημιουργίας Υπογραφής, Ηλεκτρονική Ανταλλαγή Εγγράφων, Μητρώο Πολιτών, Κάρτα Πολίτη, Εθνική Ψηφιακή Στρατηγική, Κεντρικό Σύστημα Ηλεκτρονικής Διακίνησης Εγγράφων, Διαλειτουργικότητα μεταξύ Φορέων.

ABSTRACT

This paper was designed to present and analyze a contemporary issue concerning the facilitation of citizens in their transactions with the state mechanism, **the electronic document exchange and the digital signature in the Public Sector.**

The first chapter introduces the definitions of e-Government and Information and Communication Technologies (ICT) in Greece, and we analyze the basic principles and the objectives of the e-Government strategy's plan 2014-2020.

In the second chapter, reference is made to the definition of an electronic document, the definition of digital signature and its encryption methods. Subsequently, the steps of creating a digital signature are analyzed and information about the public key certificate, the public key infrastructure (PKI) and the categories of Usb tokens is provided.

The third chapter describes in detail the process of issuing an electronic signature via the Public Key Infrastructure (PKI) of HARICA. It also describes the process of the digital signing of a file and an e-mail message.

At the fourth chapter is briefly presented the process of issuing an electronic signature via ERMIS portal.

The fifth chapter analyzes the future of Information Systems, the Civils' Registration System and the Citizen's Card for the purpose of flexible and efficient public administration.

Finally, the sixth chapter presents the very promising plan of the Central Electronic Document Handling System (ETS), its advantages and its basic elements of its architecture.

KEY WORDS: Digital signature, Personal Digital Certificate, Public Key Certificate, Usb token, Electronic Document Exchange, Civil Registration System, Citizen Card, National Digital Strategy, Central Electronic Document Handling System, Interoperability between Organizations.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον επίκουρο καθηγητή του Τμήματος Πληροφορικής με Εφαρμογές στη Βιοϊατρική του Πανεπιστημίου Θεσσαλίας, κ. Αθανάσιο Λουκόπουλο για την πολύτιμη καθοδήγησή του καθώς και τη βοήθεια που μου προσέφερε κατά την εκπόνηση αυτής της εργασίας. Θέλω επίσης να ευχαριστήσω τους καθηγητές της επιτροπής καθώς και τους υπόλοιπους καθηγητές του ΔΠΜΣ για τη συμβολή τους στην εκπαίδευση μου κατά τη διάρκεια της φοίτησής μου και για τα χρήσιμα για το μέλλον μου εφόδια που μου παρείχαν.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ i

ABSTRACT iii

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ ix

ΠΡΟΛΟΓΟΣ 1

ΚΕΦΑΛΑΙΟ 1: ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΑΙ ΤΠΕ 3

1.1. ΕΙΣΑΓΩΓΗ 3

1.2. ΟΡΙΣΜΟΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΚΑΙ ΤΠΕ 3

1.3. ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΣΤΡΑΤΗΓΙΚΗΣ ΓΙΑ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ 2014-2020 4

1.4. ΣΤΟΧΟΙ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΓΙΑ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ 2014-2020 6

1.4.1. Εκσυγχρονισμός Κράτους και Διοίκησης 7

1.4.2. Επανασύνδεση Πολίτη με Κράτος και Διοίκηση 8

1.4.3. Συντονισμός Οριζοντίων Πολιτικών ΤΠΕ στη Δημόσια Διοίκηση 9

ΚΕΦΑΛΑΙΟ 2: ΗΛΕΚΤΡΟΝΙΚΗ - ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ 10

2.1. ΕΙΣΑΓΩΓΗ 10

2.2. ΟΡΙΣΜΟΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΓΡΑΦΟΥ - ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ 10

2.3. ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗ 12

2.3.1. Συμμετρική Κρυπτογράφηση 14

2.3.2. Μη συμμετρική Κρυπτογράφηση - Ασύμμετρη Κρυπτογραφία 16

2.3.3. Τριμερής Ασύμμετρη Κρυπτογραφία 19

2.3.4. Λογισμικό Κρυπτογράφησης PGP (Pretty Good Privacy) 20

2.4. ΣΤΑΔΙΑ ΔΗΜΙΟΥΡΓΙΑΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ 20

2.5. ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ - ΨΗΦΙΑΚΟ ΠΙΣΤΟΠΟΙΗΤΙΚΟ 24

2.6. ΑΣΦΑΛΗΣ ΔΙΑΤΑΞΗ ΔΗΜΙΟΥΡΓΙΑΣ ΥΠΟΓΡΑΦΗΣ (ΑΔΔΥ) 25

2.6.1. Έξυπνη Κάρτα (Smart Card) 25
2.6.2. USB Token 28
2.7. ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (ΥΔΚ) 29
2.7.1. Ορισμοί και ρόλοι της Υποδομής Δημοσίου Κλειδιού (ΥΔΚ) 30
ΚΕΦΑΛΑΙΟ 3: ΔΙΑΔΙΚΑΣΙΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ ΜΕΣΩ ΤΗΣ HARICA .. 36
3.1. ΕΙΣΑΓΩΓΗ 36
3.2. ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ HARICA 36
3.3. ΡΥΘΜΙΣΗ ΣΥΣΚΕΥΗΣ ΓΙΑ ΧΡΗΣΗ ΤΗΣ ΕΞΥΠΝΗΣ ΚΑΡΤΑΣ -ΑΚΑΔΗΜΑΪΚΗΣ ΤΑΥΤΟΤΗΤΑΣ 37
3.4. ΔΙΑΔΙΚΑΣΙΑ ΕΚΔΟΣΗΣ ΨΗΦΙΑΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΤΥΠΟΥ CLASS A 42
3.5. ΈΛΕΓΧΟΣ ΑΠΟΘΗΚΕΥΣΗΣ ΠΡΟΣΩΠΙΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΕ ΛΟΓΙΣΜΙΚΟ WINDOWS 59
3.6. ΈΛΕΓΧΟΣ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΗΝ ΑΚΑΔΗΜΑΪΚΗ ΤΑΥΤΟΤΗΤΑ 61
3.7. ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ PDF ΑΡΧΕΙΟΥ ΜΕ ΤΗ ΧΡΗΣΗ ΤΟΥ ADOBE READER .. 64
3.8. ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΜΗΝΥΜΑΤΟΣ ΜΕΣΩ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ΜΕ MOZILLA THUNDERBIRD 74
ΚΕΦΑΛΑΙΟ 4: ΣΥΣΤΗΜΑ ΕΚΔΟΣΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ ΜΕΣΩ ΤΗΣ ΠΥΛΗΣ ΕΡΜΗΣ 83
4.1. ΕΙΣΑΓΩΓΗ 83
4.2. ΟΡΙΣΜΟΣ ΤΗΣ ΠΥΛΗΣ ΕΡΜΗΣ 83
4.3. ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΒΟΛΗ ΑΙΤΗΜΑΤΟΣ ΕΚΔΟΣΗΣ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΜΕΣΩ ΤΗΣ ΠΥΛΗΣ ΕΡΜΗΣ 84
ΚΕΦΑΛΑΙΟ 5: ΜΗΤΡΩΟ ΠΟΛΙΤΩΝ ΚΑΙ ΚΑΡΤΑ ΠΟΛΙΤΗ 93
5.1. ΕΙΣΑΓΩΓΗ 93
5.2. ΜΗΤΡΩΟ ΠΟΛΙΤΩΝ 93
5.3. ΚΑΡΤΑ ΠΟΛΙΤΗ - ΝΕΑ ΤΑΥΤΟΤΗΤΑ 94

5.3.1. Δομή και Τεχνικά Χαρακτηριστικά της Κάρτας Πολίτη 95
ΚΕΦΑΛΑΙΟ 6: ΗΛΕΚΤΡΟΝΙΚΗ ΑΝΤΑΛΛΑΓΗ ΕΓΓΡΑΦΩΝ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ 99
6.1. ΕΙΣΑΓΩΓΗ 99
6.2. ΚΕΝΤΡΙΚΟ ΣΥΣΤΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΙΝΗΣΗΣ ΕΓΓΡΑΦΩΝ (ΣΗΔΕ) 99
6.2.1. Πλεονεκτήματα του ΣΗΔΕ 100
6.2.2. Αρχιτεκτονική συστήματος ΣΗΔΕ 100
6.2.2.1. Σύστημα Απομακρυσμένων Ψηφιακών Υπογραφών (ΣΨΥ) 101
6.2.2.2. Σύστημα Διακίνησης Εγγράφων, Δρομολόγησης και Διαλειτουργικότητας (ΣΔΔΔ) 102
6.2.2.3.Συστήματα Ηλεκτρονικής Διακίνησης Εγγράφων Φορέων (ΣΗΔΕ-Φ) 102
6.2.2.4. Εργαλείο Υποστήριξης Χρηστών (Help Desk Software Tool) 103
6.2.2.5. Βάση δεδομένων 103
6.2.2.6. Σημεία διασύνδεσης με τα τοπικά ΣΗΔΕ (ΣΗΔΕ 1,2,...,N) 103
ΚΕΦΑΛΑΙΟ 7: ΣΥΜΠΕΡΑΣΜΑΤΑ 105
ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΝΑΦΟΡΕΣ 107

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1: Διαδικασία Κρυπτογράφησης 13
Εικόνα 2: Διαδικασία Αποκρυπτογράφησης 13
Εικόνα 3: Συμμετρική κρυπτογραφία 15
Εικόνα 4: Εξασφάλιση εμπιστευτικότητας (1) 17
Εικόνα 5: Εξασφάλιση εμπιστευτικότητας (2) 17
Εικόνα 6: Πιστοποίηση ταυτότητας αποστολέα (1) 18
Εικόνα 7: Πιστοποίηση ταυτότητας αποστολέα (2) 18
Εικόνα 8: Διαδικασία δημιουργίας ηλεκτρονικής υπογραφής 22
Εικόνα 9: Διαδικασία επαλήθευσης ηλεκτρονικής υπογραφής 23
Εικόνα 10: Εμπρόσθια όψη έξυπνης κάρτας 26
Εικόνα 11: Οπίσθια όψη έξυπνης κάρτας 27
Εικόνα 12: Εμπρόσθια όψη αναγνώστη έξυπνης κάρτας 27
Εικόνα 13: Οπίσθια όψη αναγνώστη έξυπνης κάρτας 28
Εικόνα 14: Εμπρόσθια όψη USB token, Safenet 5100 28
Εικόνα 15: Οπίσθια όψη USB token, Safenet 5100 29
Εικόνα 16: Αρχιτεκτονική PKI 32
Εικόνα 17: Γενικές πληροφορίες πιστοποιητικού 33
Εικόνα 18:Λεπτομέρειες πιστοποιητικού 34
Εικόνα 19: Διαδρομή πιστοποίησης 35
Εικόνα 20: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (1) 38
Εικόνα 21: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (2) 38
Εικόνα 22: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (3) 39
Εικόνα 23: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (4) 40
Εικόνα 24: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (5) 40
Εικόνα 25: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (6) 41
Εικόνα 26: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (7) 41
Εικόνα 27: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (8) 42
Εικόνα 28: Επαληθευτής Google 44

Εικόνα 29: Επαληθευτής Google - Κωδικός HARICA 45
Εικόνα 30: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (1)..... 45
Εικόνα 31: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (2)..... 46
Εικόνα 32: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (3)..... 46
Εικόνα 33: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (4)..... 47
Εικόνα 34: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (5)..... 48
Εικόνα 35: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (6)..... 48
Εικόνα 36: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (7)..... 49
Εικόνα 37: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (8)..... 49
Εικόνα 38: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (9)..... 50
Εικόνα 39: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (10)..... 51
Εικόνα 40: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (11)..... 51
Εικόνα 41: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (12)..... 52
Εικόνα 42: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (13)..... 53
Εικόνα 43: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (14)..... 53
Εικόνα 44: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (15)..... 54
Εικόνα 45: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (16)..... 55
Εικόνα 46: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (17)..... 55
Εικόνα 47: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (18)..... 56
Εικόνα 48: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (19)..... 57
Εικόνα 49: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (20)..... 57
Εικόνα 50: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (21)..... 58
Εικόνα 51: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (22)..... 59
Εικόνα 52: Έλεγχος Αποθήκευσης Προσωπικού Πιστοποιητικού - Επιλογές Internet..... 60
Εικόνα 53: Έλεγχος Αποθήκευσης Προσωπικού Πιστοποιητικού - Επιλογές Internet - Περιεχόμενο - Πιστοποιητικά 60
Εικόνα 54: Έλεγχος Αποθήκευσης Προσωπικού Πιστοποιητικού - Επιλογές Internet - Προσωπικά στοιχεία..... 61
Εικόνα 55: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (1)..... 62

Εικόνα 56: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (2)..... 62
Εικόνα 57: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (3)..... 63
Εικόνα 58: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (4)..... 63
Εικόνα 59: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (5)..... 64
Εικόνα 60: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (1)..... 65
Εικόνα 61: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (2)..... 66
Εικόνα 62: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (3)..... 67
Εικόνα 63: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (4)..... 67
Εικόνα 64: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (5)..... 68
Εικόνα 65: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (6)..... 69
Εικόνα 66: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (7)..... 70
Εικόνα 67: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (8)..... 70
Εικόνα 68: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (9)..... 71
Εικόνα 69: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (10)..... 71
Εικόνα 70: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (11)..... 72
Εικόνα 71: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (12)..... 72
Εικόνα 72: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (13)..... 73
Εικόνα 73: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (14)..... 74
Εικόνα 74: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (15)..... 74
Εικόνα 75: Εξαγωγή ψηφιακού πιστοποιητικού από την ακαδημαϊκή ταυτότητα (1) 75
Εικόνα 76: Εξαγωγή ψηφιακού πιστοποιητικού από την ακαδημαϊκή ταυτότητα (2) 76
Εικόνα 77: Εξαγωγή ψηφιακού πιστοποιητικού από την ακαδημαϊκή ταυτότητα (3) 76
Εικόνα 78: Εξαγωγή ψηφιακού πιστοποιητικού από την ακαδημαϊκή ταυτότητα (4) 77
Εικόνα 79: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (1)..... 78
Εικόνα 80: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (2)..... 79
Εικόνα 81: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (3)..... 80

Εικόνα 82: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (4) 80
Εικόνα 83: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (5) 81
Εικόνα 84: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (6) 82
Εικόνα 85: Συνοπτική περιγραφή διαδικασίας έκδοσης ψηφιακών πιστοποιητικών 85
Εικόνα 86: Σύνδεση στη Πύλη ΕΡΜΗΣ 86
Εικόνα 87: Είσοδος στην Πύλη ΕΡΜΗΣ 86
Εικόνα 88: Οθόνη εισαγωγής κωδικών 87
Εικόνα 89: Εξουσιοδότηση 87
Εικόνα 90: Συμπλήρωση email 88
Εικόνα 91: Όνομα χρήστη πύλης ΕΡΜΗΣ 89
Εικόνα 92: Πίνακας Ελέγχου πύλης ΕΡΜΗΣ 89
Εικόνα 93: Πίνακας Ελέγχου - Διαχείριση προσωπικών ψηφιακών πιστοποιητικών 90
Εικόνα 94: Ηλεκτρονική Υποβολή Αιτήματος Έκδοσης Ψηφιακών Πιστοποιητικών 91
Εικόνα 95: Ολοκλήρωση Υποβολής Αιτήματος Έκδοσης Ψηφιακών Πιστοποιητικών 92
Εικόνα 96: Εμπρόσθια όψη Κάρτας Πολίτη 96
Εικόνα 97: Οπίσθια όψη Κάρτας Πολίτη 97
Εικόνα 98: Αρχιτεκτονική ΣΗΔΕ 101

ΠΡΟΛΟΓΟΣ

Σε παγκόσμιο επίπεδο, η αναβάθμιση του ρόλου της Δημόσιας Διοίκησης είναι αναγκαία προϋπόθεση για την παραγωγική ανασυγκρότηση της κάθε χώρας και για την αναπτυξιακή προοπτική της.

Όλα αυτά τα χρόνια στον Ελλαδικό χώρο, η Δημόσια Διοίκηση έχει επιδείξει σημαντικές και σοβαρές αδυναμίες στην λειτουργία της. Οι αδυναμίες αυτές έγκεινται στον συντονισμό των διοικητικών υπηρεσιών, τις γραφειοκρατικές καθυστερήσεις, αδυναμίες στη διαχείριση του ανθρώπινου δυναμικού και την αξιοποίηση νέων τεχνολογιών.

Από την άλλη μεριά, η εξέλιξη της τεχνολογίας και η ηλεκτρονική επικοινωνία καθιστούν επιτακτική ανάγκη τον εκσυγχρονισμό της Δημόσιας Διοίκησης. Είναι αναγκαίος ο εκσυγχρονισμός των ηλεκτρονικών υπηρεσιών αλλά και η αναβάθμιση των ηλεκτρονικών συναλλαγών των πολιτών με τον κρατικό μηχανισμό, ώστε να λάβουν χώρα οι κατάλληλες οι μεταρρυθμίσεις και να προχωρήσει η εξυγίανση του Δημόσιου Τομέα.

Όπως θα αναλυθεί στην παρακάτω διπλωματική, μέσω των ψηφιακών υπογραφών και της ηλεκτρονικής έκδοσης και διακίνησης εγγράφων, αναβαθμίζεται και απλουστεύεται κατά πολύ η εργασιακή καθημερινότητα των υπαλλήλων. Επιτυγχάνεται έτσι, σημαντική μείωση κόστους, εξοικονόμηση χρόνου και διευκόλυνση στην επικοινωνία μεταξύ των πολιτών.

Προς την κατεύθυνση αυτή, σχεδιάστηκε το πολλά υποσχόμενο έργο του Κεντρικού Συστήματος Ηλεκτρονικής Διακίνησης Εγγράφων (ΣΗΔΕ) που αφορά στην διακίνηση και δρομολόγηση των εγγράφων, μέσω ψηφιακών υπογραφών, μεταξύ των φορέων του δημόσιου τομέα. Το κράτος, σε στενή συνεργασία με όλα τα Υπουργεία, οδηγείται ολοταχώς στην ψηφιακή ανάπτυξη της χώρας προς όφελος όλων των πολιτών.

Ο κύριος στόχος είναι να δημιουργηθεί μία νέα σχέση εμπιστοσύνης, μεταξύ κράτους και πολιτών, με διαδικασίες που προάγουν την διαφάνεια και την αξιοκρατία. Η Ελλάδα εισέρχεται σε μία νέα εποχή, εναρμονίζεται και ανταποκρίνεται στις νέες ψηφιακές προκλήσεις, συμβαδίζοντας με τα Ευρωπαϊκά Πρότυπα, με αέρα ανανέωσης και εκσυγχρονισμού.

ΚΕΦΑΛΑΙΟ 1: ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ ΚΑΙ ΤΠΕ

1.1. ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό θα αναφερθούμε στον ορισμό της Ηλεκτρονικής Διακυβέρνησης και των Τεχνολογιών της Πληροφορίας και της Επικοινωνίας - ΤΠΕ στην Ελλάδα. Στη συνέχεια, θα αναλύσουμε τις βασικές αρχές και τους στόχους της στρατηγικής του έργου της Ηλεκτρονικής Διακυβέρνησης 2014-2020, με σκοπό τον εκσυγχρονισμό του Κράτους και της Δημόσιας Διοίκησης.

1.2. ΟΡΙΣΜΟΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΚΑΙ ΤΠΕ

Ο όρος **Ηλεκτρονική Διακυβέρνηση (e-government)**[1] αναφέρεται στην χρησιμοποίηση των εφαρμογών των τεχνολογιών της πληροφορικής και των υπολογιστών στην Δημόσια Διοίκηση.

Ο όρος **Τεχνολογίες της Πληροφορίας και της Επικοινωνίας - ΤΠΕ**[2] (αγγ. **IT** ή **ICT)** αναφέρεται στις μεθόδους και εφαρμογές της σύγχρονης τεχνολογίας που χρησιμοποιούνται για την διαχείριση πληροφοριακών υπολογιστικών συστημάτων, με κύριο μέσο τον υπολογιστή.

Η Ηλεκτρονική Διακυβέρνηση[3] (e-Government), με αρωγό τις Τεχνολογίες Πληροφοριών και Επικοινωνιών (ΤΠΕ), έχει ως κύριο στόχο να αλλάξει αλλά και να αναβαθμίσει όλες τις παρεσχεθείσες υπηρεσίες προς τους πολίτες, έτσι ώστε η Δημόσια Διοίκηση που ασκείται να γίνει αποτελεσματικότερη.

Στόχος της είναι η διασύνδεση πολιτών και κράτους με απώτερο σκοπό την ουσιαστική εξυπηρέτηση της καθημερινότητας των πολιτών και την ικανοποίησης των αναγκών τους.

Σύμφωνα με το Άρθρο 5Α, Σύνταγμα της Ελλάδας, «***Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους***».

[1] https://en.wikipedia.org/wiki/E-government

[2] https://en.wikipedia.org/wiki/Information_technology

[3] http://www.minadmin.gov.gr/?page_id=12126

Αρμόδιο όργανο της κυβέρνησης για να ασκηθεί η κυβερνητική πολιτική όσον αφορά την αξιοποίηση των ΤΠΕ στην Δημόσια Διοίκηση είναι το Υπουργείο Διοικητικής Ανασυγκρότησης[4].

1.3. ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΣΤΡΑΤΗΓΙΚΗΣ ΓΙΑ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ 2014-2020

Στην ενότητα αυτή, θα αναφερθούμε στις βασικές αρχές της στρατηγικής για την Ηλεκτρονική διακυβέρνηση στην Ελλάδα όπως αυτή παρουσιάστηκε στο «**Σχέδιο Δράσης Ηλεκτρονικής Διακυβέρνησης 2014-2020**»[5] του Υπουργείου Διοικητικής Μεταρρύθμισης. Αναλυτικά αυτές είναι:

1. Διαλειτουργικότητα

Όλα τα πληροφοριακά συστήματα θα έχουν την ικανότητα να συνδέονται και να επικοινωνούν πλήρως μεταξύ τους, με σκοπό την ανταλλαγή δεδομένων, βασισμένα σε συμβατά και αποδεκτά πρότυπα και ανεξαρτήτως λειτουργικού και λογισμικού συστήματος. Κατ' επέκταση, ο πολίτης δεν θα συμμετέχει στην όλη διαδικασία από φορέα σε φορέα, παρά μόνο στο τελικό στάδιο παραλαβής της υπηρεσίας που αιτείται.

2. Συμμόρφωση ή αιτιολόγηση

Κάθε κανόνας και διαδικασία που χρησιμοποιείται πρέπει να έχει συμβατότητα με τις αρχές της εν λόγω στρατηγικής. Εάν κάποια διαδικασία διαφοροποιείται, θα πρέπει να δικαιολογεί τους λογούς της μη συμμόρφωσής της, με πλήρως τεκμηριωμένη ανάλυση. Επίσης, στην ανάλυση θα πρέπει να παρουσιάζεται και η διαδικασία επίτευξης της συμμόρφωσης με στόχους και συγκεκριμένο χρονοδιάγραμμα.

[4] http://www.minadmin.gov.gr

[5] http://www.minadmin.gov.gr/wp-content/uploads/20140415_egov_strategy.pdf

3. Ενοποίηση

Όλο το υλικό (hardware) - εξοπλισμός και το λογισμικό σύστημα (software) που χρησιμοποιούνται στο έργο της ηλεκτρονικής διακυβέρνησης, θα τοποθετηθούν σε κοινά κέντρα δεδομένων. Η πρόσβαση σε αυτά θα είναι ενιαία, με κοινούς κανόνες και διαδικασίες.

4. Εξοικονόμηση - Μη επανάληψη

Μέσω των δράσεων της Ηλεκτρονικής Διακυβέρνησης θα εξοικονομηθούν πολύτιμοι πόροι για τη Δημόσια Διοίκηση και αντίστοιχος χρόνος για τον πολίτη. Η τεκμηρίωση της μη σπατάλης πόρων θα πρέπει να προκύπτει μέσω μελετών ανάλυσης κόστους - οφέλους, συμπεριλαμβανομένου και του χρόνου απόσβεσης της διαδικασίας. Επίσης, κάθε δράση θα πρέπει να υλοποιηθεί μία φορά και να μην υπάρξει αναγκαιότητα επανάληψης.

5. Μοναδική καταχώρηση δεδομένων

Η διαδικασία καταχώρησης των πληροφοριών (δεδομένων) για κάθε πολίτη θα πραγματοποιηθεί μία και μόνο φορά και θα διατηρηθεί σε ένα από τα Μητρώα των συστημάτων της Δημόσιας Διοίκησης. Η πληροφορία αυτή θα είναι στην διάθεση σε όλους τους υπόλοιπους αρμόδιους φορείς.

6. Εφικτότητα - Βιωσιμότητα

Για να μπορεί η Δημόσια Διοίκηση να υλοποιήσει το έργο της Ηλεκτρονικής Διακυβέρνησης, κρίνεται αναγκαία η διασφάλιση της εφικτότητας - δυνατότητας πραγματοποίησης και της βιωσιμότητας - ύπαρξης των δράσεων του έργου.

7. Διαφάνεια - Ανάκτηση Εμπιστοσύνης

Κύρια αρχή είναι η ενίσχυση της διαφάνειας, της ακεραιότητάς αλλά και της αποδοτικότητας στις συναλλαγές των πολιτών, με γνώμονα τον σωστό σχεδιασμό των δράσεων της ηλεκτρονικής διακυβέρνησης, έτσι ώστε να ανακτηθεί η εμπιστοσύνη των πολιτών.

8. <u>Προσβασιμότητα (e-accessibility)</u>

Η αρχή της προσβασιμότητάς ορίζει την πρόσβαση χωρίς περιορισμούς σε δικτυακούς τόπους της Δημόσιας Διοίκησης για ευπαθείς ομάδες, όπως τα άτομα με αναπηρία και οι ψηφιακά αναλφάβητοι. Θα εφαρμοστούν όλες οι προδιαγραφές προσβασιμότητας, σε συμμόρφωση με τα διεθνή πρότυπα που χρησιμοποιούνται, και θα ενσωματωθούν παράλληλα σε όλους τους δικτυακούς τόπους.

9. <u>Ασφάλεια - Ιδιωτικότητα</u>

Οι αποθηκευμένες πληροφορίες, οι δομές και οι διαδικασίες της ηλεκτρονικής διακυβέρνησης τα συστήματα και τα δίκτυα της Δημόσιας Διοίκησης πρέπει να διέπονται από κανόνες ασφάλειας, ούτως ώστε να μην υποπέσουν σε παραβίαση, αναρμόδια πρόσβαση ή αλλοίωση. Επιπρόσθετα, δεν θα πρέπει να γίνει χρήση των προσωπικών δεδομένων των πολιτών από μη εξουσιοδοτημένα άτομα, εξασφαλίζοντας έτσι την προστασία της ιδιωτικότητάς τους.

10. <u>Συμμετοχή πολιτών</u>

Η συμμετοχή των πολιτών είναι απαραίτητη για τη λήψη κυβερνητικών αποφάσεων όπως επίσης και για την αξιολόγηση των υπηρεσιών που παρέχει η δημόσια διοίκηση.

1.4. ΣΤΟΧΟΙ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΓΙΑ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ 2014-2020

Στην ενότητα αυτή, θα αναφερθούμε στους στόχους της στρατηγικής για την Ηλεκτρονική Διακυβέρνηση 2014-2020. Οι στόχοι αυτοί χωρίζονται σε 3 μεγάλες κατηγορίες και αναλύονται λεπτομερώς παρακάτω:

1. **Εκσυγχρονισμός Κράτους και Διοίκησης**
2. **Επανασύνδεση Πολίτη με Κράτος και Διοίκηση**
3. **Συντονισμός Οριζοντίων Πολιτικών ΤΠΕ στη Δημόσια Διοίκηση**

1.4.1. Εκσυγχρονισμός Κράτους και Διοίκησης

- **1ος Στόχος - Απλούστευση Διαδικασιών με χρήση ΤΠΕ**

Κατά την αίτηση ενός πιστοποιητικού από μία δημόσια υπηρεσία, θα εφαρμόζεται η ψηφιοποίηση και η αυτεπάγγελτη αναζήτησή του, χωρίς να είναι αναγκαία η ανθρώπινη παρέμβαση. Μέσω της επικοινωνίας όλων των πληροφοριακών συστημάτων, σταδιακά θα εξαλειφθεί η υποχρεωτική διαδικασία των ενδιάμεσων σταδίων και θα ελαττωθεί ο αριθμός των δικαιολογητικών που απαιτούνται.

Θα απλουστευτούν οι υπηρεσίες έτσι ώστε να διατηρηθούν μόνο αυτές που είναι απαραίτητες για την ηλεκτρονική παροχή των εγγράφων. Επίσης, τα ψηφιοποιημένα έγγραφα που θα παρέχονται θα έχουν νόμιμη ισχύ και δεν θα χρειάζεται να επικυρώνονται.

- **2ος Στόχος - Ηλεκτρονική διαχείριση εγγράφων - Ψηφιοποίηση διεργασιών**

Θα εγκατασταθεί ένα κεντρικό σύστημα διακίνησης, δρομολόγησης και αρχειοθέτησης εγγράφων, μεταξύ Υπουργείων και φορέων της Δημόσιας Διοίκησης. Η μεταξύ τους επικοινωνία θα γίνεται ηλεκτρονικά και τα έγγραφα που θα χρησιμοποιούνται θα είναι βασισμένα σε κοινώς αποδεκτά πρότυπα.

Θα ξεκινήσει η διάθεση ψηφιακών - ηλεκτρονικών υπογραφών (αναλύονται παρακάτω) σε στελέχη του Δημοσίου, η οποία θα συντελέσει στην ηλεκτρονική διεκπεραίωση των εγγράφων και τη ψηφιοποίηση των διεργασιών.

- **3ος Στόχος - Ενιαία διαχείριση πόρων Δημόσιας Διοίκησης**

Θα υλοποιηθεί ένα ολοκληρωμένο σύστημα όσον αφορά την διαχείριση των πόρων της Δημόσιας Διοίκησης και θα εφαρμοστεί στις πληροφοριακές υποδομές, στις υπηρεσίες και στο ανθρώπινο δυναμικό του Δημοσίου.

1.4.2. Επανασύνδεση Πολίτη με Κράτος και Διοίκηση

- **4ος Στόχος - Ενιαία διαχείριση σχέσεων κράτους πολίτων και επιχειρήσεων**

Όλες οι συναλλαγές του πολίτη με το Δημόσιο, θα αντιμετωπίζονται ενιαία και συνολικά, σε όλο το εύρος πρόσβασής τους (διαδίκτυο, τηλεφωνική επικοινωνία, φυσική παρουσία).

- **5ος Στόχος - Δημιουργία ενιαίου σημείου πρόσβασης στις υπηρεσίες του Δημόσιου Τομέα**

Για την εξυπηρέτηση ενός αιτήματος συναλλαγής με το Δημόσιο, ο πολίτης θα χρησιμοποιεί ένα κοινό σημείο πρόσβασης από όπου και θα δέχεται τις τελικές υπηρεσίες που θα αιτείται. Η διαδικασία επεξεργασίας του αιτήματος δεν θα είναι ένα θέμα που θα απασχολεί τον πολίτη, καθώς η δρομολόγησή του θα γίνεται εσωτερικά και μεταξύ των φορέων της Δημόσιας Διοίκησης.

Το κοινό σημείο πρόσβασης θα είναι μία Κεντρική Διαδικτυακή Πύλη Ενιαίας Πρόσβασης (Πύλη ΕΡΜΗΣ) η οποία, μέσω ενός εύχρηστου και φιλικού περιβάλλοντος, θα παρέχει σχετικές πληροφορίες στους πολίτες για όλες τις ηλεκτρονικές συναλλαγές τους με το Δημόσιο.

- **6ος Στόχος - Αυθεντικοποίηση πολιτών**

Οι κωδικοί που χρησιμοποιούνται για την αυθεντικοποίηση των πολιτών όπως ο ΑΜΚΑ, ο ΑΦΜ, ο ΑΔΤ - Αριθμός Δελτίου Ταυτότητας θα διασυνδεθούν μεταξύ τους.

Επίσης, για την ευκολία των πολιτών, η αυθεντικοποίηση θα γίνεται και από άλλες συσκευές όπως το κινητό τηλέφωνο, έξυπνη κάρτα (αναλύεται παρακάτω) μέσω κατάλληλων υποδομών.

- **7ος Στόχος - Συμμετοχική Δημοκρατία**

Εξασφαλίζεται η πρόσβαση και η συμμετοχή των πολιτών σε όλους τους τομείς της Δημόσιας Διοίκησης. Επιπρόσθετα, μέσω της ηλεκτρονικής διαδικασίας εξυπηρέτησης, μειώνεται η ανάγκη των προσωπικών επαφών πολίτη και κράτους, συμβάλλοντας στην μείωση της διαφθοράς και προώθηση της διαφάνειας.

- **8ος Στόχος - Ψηφιακή ένταξη και ψηφιακός αλφαβητισμός**

Μέσω της τεχνολογικής υποδομής και της υλοποίησης επιμορφωτικών προγραμμάτων κατάρτισης, θα μειωθεί το ποσοστό ψηφιακού αναλφαβητισμού θα ενισχυθεί η ψηφιακή ένταξη.

1.4.3. Συντονισμός Οριζοντίων Πολιτικών ΤΠΕ στη Δημόσια Διοίκηση

- **9ος Στόχος - Διασύνδεση βασικών Μητρώων Δημόσιας Διοίκησης**

Θα διασυνδεθούν τα κύρια Μητρώα όπως το Μητρώο Αστυνομικών Ταυτοτήτων, το Μητρώο Ασφαλισμένων, το Μητρώο Φορολογουμένων, το Δημοτολόγιο και θα διαλειτουργούν μεταξύ τους, ακολουθώντας κοινά πρότυπα .

- **10ος Στόχος - Ανοιχτή διάθεση δημόσιας πληροφορίας**

Θα υπάρξει καταγραφή του συνόλου των δεδομένων - πληροφοριών κάθε δημόσιου φορέα και ανοικτής διάθεσής τους[6].

[6] http://www.data.gov.gr

ΚΕΦΑΛΑΙΟ 2: ΗΛΕΚΤΡΟΝΙΚΗ - ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

2.1. ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό θα δούμε κάποιες πληροφορίες αναφορικά με τον ορισμό του ηλεκτρονικού εγγράφου, τον ορισμό της ηλεκτρονικής υπογραφής και τις μεθόδους κρυπτογράφησής της. Στη συνέχεια θα αναλύσουμε τα στάδια δημιουργίας ψηφιακής υπογραφής και θα δούμε πληροφορίες σχετικά με το πιστοποιητικό δημόσιου κλειδιού, την Υποδομή Δημοσίου Κλειδιού (ΥΔΚ) και τις κατηγορίες Ασφαλών Διατάξεων Δημιουργίας Υπογραφής (ΑΔΔΥ).

2.2. ΟΡΙΣΜΟΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΓΡΑΦΟΥ - ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ

Με τον όρο **ηλεκτρονικό έγγραφο** νοείται «***κάθε μέσο, το οποίο χρησιμοποιείται από υπολογιστικό - πληροφοριακό σύστημα, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων που δεν μπορούν να αναγνωστούν άμεσα, όπως και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό, στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφόσον το εν λόγω περιεχόμενο επιφέρει έννομες συνέπειες ή προορίζεται ή είναι πρόσφορο να αποδείξει γεγονότα που μπορούν να έχουν έννομες συνέπειες***», σύμφωνα με το άρθρο 3 του Νόμου 3979/2001.

Ως **ηλεκτρονικό δημόσιο έγγραφο** νοείται «***κάθε ηλεκτρονικό έγγραφο με την έννοια του άρθρου 3 του Ν. 3979/2011 που εκδίδεται από δημόσια υπηρεσία ή φορέα από το οποίο προκύπτει με μηχαναγνώσιμο τρόπο η εκδούσα αρχή, η ημερομηνία έκδοσης και είναι δυνατή η ανίχνευση οποιασδήποτε αλλοίωσης του ηλεκτρονικού εγγράφου μετά την έκδοση ή υπογραφή του***», σύμφωνα με το άρθρο 1 του Φ.Ε.Κ. 1317/Β'/23.04.2012.

Με τον όρο **ηλεκτρονική υπογραφή** νοούνται τα ***«δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και χρησιμοποιούνται ως μέθοδο απόδειξης της γνησιότητας***», σύμφωνα με το άρθρο 2 του Π.Δ. 150/2001.

Συνεχίζοντας στο ίδιο άρθρο 2 του Π.Δ. 150/2001, **προηγμένη ηλεκτρονική υπογραφή** ή **ψηφιακή υπογραφή** είναι η ***«ηλεκτρονική υπογραφή, που πληροί τους εξής όρους:***

α) συνδέεται μονοσήμαντα με τον υπογράφοντα,

β) είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος

γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και

δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται, κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων».

Ως εγκεκριμένη ηλεκτρονική υπογραφή ορίζεται η ***«προηγμένη ηλεκτρονική υπογραφή που δημιουργείται από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής και η οποία βασίζεται σε πιστοποιητικό ηλεκτρονικής υπογραφής»***, σύμφωνα με το άρθρο 3 του Κανονισμού (ΕΕ) 910/2014.

Συνοπτικά, η ηλεκτρονική ή ψηφιακή υπογραφή[7] είναι ένα σύνολο δεδομένων σε ψηφιακή μορφή που χρησιμοποιούνται για την απόδειξη της αυθεντικότητας και της εγκυρότητας ενός μηνύματος.

Οι απαιτήσεις που πρέπει να πληρούνται για την ηλεκτρονική - ψηφιακή υπογραφή είναι οι:

1. Εξασφάλιση της ακεραιότητας της πληροφορίας (integrity), δηλαδή ότι το μήνυμα το οποίο έστειλε ο αποστολέας/υπογράφων είναι αυτό το οποίο λαμβάνει ο παραλήπτης, χωρίς να έχει υποστεί αλλοίωση ή μετατροπή στα δεδομένα του.

2. Πιστοποίηση της αυθεντικότητας του αποστολέα (authentication), δηλαδή ότι το μήνυμα που λαμβάνει ο παραλήπτης προέρχεται από τον αποστολέα/υπογράφων και όχι από κάποιον που παριστάνει τον αποστολέα.

3. Εξασφάλιση της μη αποποίησης ευθύνης (μη αποποίηση - non repudiation), δηλαδή και τα δύο μέρη που εμπλέκονται σε μία συναλλαγή να μην μπορούν να αρνηθούν ότι συμμετείχαν στην συναλλαγή.

4. Εξασφάλιση της εμπιστευτικότητας (confidentiality), δηλαδή την αποτροπή πρόσβασης σε μη εξουσιοδοτημένους χρήστες. Σε περίπτωση που υπάρχει παράνομη

[7] https://en.wikipedia.org/wiki/Digital_signature

πρόσβαση, θα πρέπει να διασφαλιστεί η αδυναμία του εισβολέα να διαβάσει το περιεχόμενό του μηνύματος.

Μέσω της χρήσης της τεχνικής της κρυπτογράφησης, η ψηφιακή υπογραφή εξασφαλίζει τις παραπάνω προϋποθέσεις. Στη συνέχεια, αναλύονται οι βασικές έννοιες της κρυπτογράφησης και οι τεχνικές της.

2.3. ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Ο όρος της **κρυπτογραφίας**[8] (προέρχεται από το συνθετικό των λέξεων «κρυπτός» και «γράφω») αναφέρεται στον τομέα της επιστήμης εκείνον που μελετά και αναπτύσσει μεθόδους κρυπτογράφησης και αποκρυπτογράφησης μηνυμάτων, με απώτερο στόχο την απόκρυψη του περιεχομένου τους. Η επιστήμη της κρυπτογραφίας είναι μία επιστήμη που ασχολείται με την κωδικοποίηση και αποκωδικοποίηση των δεδομένων, χρησιμοποιώντας τον κλάδο των μαθηματικών

Αντίστοιχα με τον όρο **κρυπτογράφηση (encryption)** αναφερόμαστε στην διαδικασία μετάδοσης ενός μηνύματος - πληροφορίας, με τρόπο τέτοιο ώστε να μπορεί να «διαβαστεί» μόνο από τον παραλήπτη της. Συνεπώς, μέσω της κρυπτογράφησης εξασφαλίζεται το απόρρητο των προσωπικών πληροφοριών.

Η διαδικασία της κρυπτογράφησης περιληπτικά έχει ως εξής:

- Η αρχική πληροφορία-κείμενο μετασχηματίζεται από τον αποστολέα σε μία μορφή μη κατανοητή για οποιονδήποτε τρίτο, με την χρήση κάποιας μαθηματικής συνάρτησης (κρυπτογραφημένο κείμενο).
- Στη συνέχεια, το κείμενο αποκρυπτογραφείται από τον παραλήπτη, ο οποίος γνωρίζει τον τρόπο κρυπτογράφησης, όπως ήταν στην αρχική του μορφή.

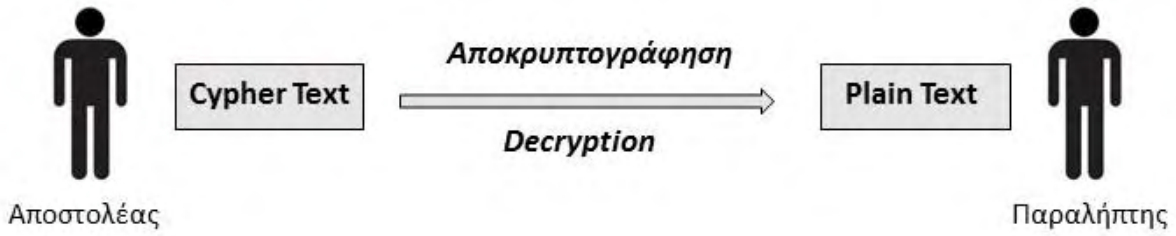
Πιο συγκεκριμένα, μέσω της **κρυπτογράφησης** επιτυγχάνεται ο μετασχηματισμός της πληροφορίας (**Απλό Κείμενο - Plain Text: PT**) σε μία μη κατανοητή μορφή (**Κρυπτογραφημένο Κείμενο - Cypher Text: CT**) χρησιμοποιώντας έναν αλγόριθμο

[8] https://en.wikipedia.org/wiki/Cryptography

(**Αλγόριθμος Κρυπτογράφησης - Cipher**) και ένα κλειδί (**Key**). Στην παρακάτω εικόνα περιγράφεται η διαδικασία της κρυπτογράφησης με ένα απλό σχήμα:

Εικόνα 1: Διαδικασία Κρυπτογράφησης

Η διαδικασία της **αποκρυπτογράφησης** λειτουργεί αντίστροφα, δηλαδή η κρυπτογραφημένη μορφή (cypher text) μετασχηματίζεται στην αρχική μορφή (plain text) χρησιμοποιώντας τον αλγόριθμο αποκρυπτογράφησης (αντίστροφος αλγόριθμος) και το αντίστοιχο κλειδί. Στην παρακάτω εικόνα περιγράφεται η διαδικασία της αποκρυπτογράφησης με ένα απλό σχήμα:



Εικόνα 2: Διαδικασία Αποκρυπτογράφησης

Η κρυπτογράφηση και η αποκρυπτογράφηση των πληροφοριών γίνεται μέσω μιας μαθηματικής συνάρτησης που ονομάζεται **αλγόριθμος κρυπτογράφησης (cipher)**. Όσο πιο πολύπλοκος είναι αυτός ο αλγόριθμος, τόσο πιο δύσκολο είναι να προσπελαστεί από κάποιον μη εξουσιοδοτημένο. Όπως αναφέρθηκε ήδη, ο αλγόριθμος κρυπτογράφησης σε συνδυασμό με ένα κλειδί (key), χρησιμοποιείται για την κρυπτογράφηση του απλού κειμένου.

Το **κλειδί κρυπτογράφησης (key)** είναι ουσιαστικά μια ακολουθία χαρακτήρων. Όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο πιο ασφαλής γίνεται η διαδικασία της κρυπτογράφησης.

Συνοψίζοντας, ο αλγόριθμος είναι η αντιμετάθεση γραμμάτων ενώ κλειδί είναι το πλήθος των θέσεων.

Η μέθοδος της κρυπτογραφίας διακρίνεται σε δύο μεγάλες κατηγορίες οι οποίες είναι:

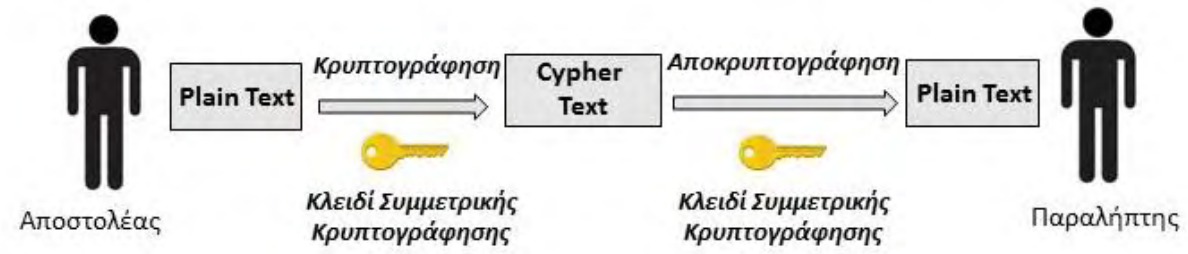
1. Η **συμμετρική κρυπτογραφία** ή κρυπτογραφία συμμετρικού κλειδιού στην οποία γίνεται χρήση του ίδιου κλειδιού τόσο για την κρυπτογράφηση που γίνεται από τον αποστολέα όσο και για την αποκρυπτογράφηση που γίνεται από τον παραλήπτη. Στην μέθοδο αυτή της συναλλαγής διασφαλίζεται η μυστικότητα του κλειδιού μεταξύ των συναλλασσόμενων. Τα μειονεκτήματά της είναι η εφαρμογή της σε περιπτώσεις με πολλούς χρήστες (για το πως θα ανταλλάσσουν μεταξύ τους το κλειδί με ασφάλεια) και ότι χρειάζεται να υπάρχουν αυξημένες απαιτήσεις ασφάλειας (για την αποθήκευση κλειδιών κ.α.)
2. **Η μη συμμετρική κρυπτογραφία** ή ασύμμετρη κρυπτογραφία ή αλλιώς (κρυπτογραφία δημοσίου κλειδιού - public key cryptography) στη οποία γίνεται χρήση δύο διαφορετικών κλειδιών τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Ο κάθε χρήστης διαθέτει δύο κλειδιά από τα οποία το μεν δημόσιο κλειδί του μπορεί να γνωστοποιηθεί σε τρίτους ενώ το ιδιωτικό του κλειδί δε διαφυλάσσεται με ασφάλεια μόνο από αυτόν. Ο αποστολέας χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη, κρυπτογραφεί το μήνυμα. Στη συνέχεια, η αποκρυπτογράφηση του μηνύματος γίνεται από το αντίστοιχο ιδιωτικό κλειδί του παραλήπτη, εφόσον αυτός είναι κάτοχος του κλειδιού.

Τέλος, υπάρχει μία ακόμη μέθοδος αυτή της **Τριμερής Ασύμμετρης Κρυπτογραφίας**, η οποία αποτελεί υποκατηγορία της ασύμμετρης κρυπτογραφίας και εφαρμόζεται στην προηγμένη ηλεκτρονική υπογραφή και πλέον στην εγκεκριμένη ηλεκτρονική υπογραφή. Στις επόμενες ενότητες περιγράφονται αναλυτικά οι παραπάνω μέθοδοι κρυπτογράφησης.

2.3.1. Συμμετρική Κρυπτογράφηση

Η συμμετρική κρυπτογραφία ή αλλιώς κρυπτογραφία συμμετρικού κλειδιού (Symmetric Cryptography) είναι η μέθοδος όπου γίνεται χρήση ενός μοναδικού κλειδιού, τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση, διασφαλίζοντας έτσι τη μυστικότητα του κλειδιού μεταξύ των συναλλασσόμενων.

Η διαδικασία κρυπτογράφησης συμμετρικού κλειδιού απεικονίζεται στο επόμενο σχήμα.



Εικόνα 3: Συμμετρική κρυπτογραφία

Μια αδυναμία αυτού του τρόπου κρυπτογράφησης είναι η ασφαλής ανταλλαγή του κλειδιού. Είναι αδύνατο να διαπιστωθεί κατά πόσο η προέλευση του μηνύματος είναι από τον αληθινό αποστολέα του ή από κάποιον που παρανόμως παριστάνει ότι είναι αυτός. Η ανταλλαγή του κλειδιού μεταξύ των συναλλασσόμενων θα πρέπει να γίνεται μέσω ασφαλούς επικοινωνίας και οι κωδικοί θα πρέπει να αποθηκεύονται με ασφάλεια, διαδικασίες που συντελούν επιπλέον στις αδυναμίες αυτής της μεθόδου.

Από την άλλη μεριά, σημαντικό πλεονέκτημα της συμμετρικής κρυπτογραφίας είναι η μείωση του χρόνου της διαδικασίας της κρυπτογράφησης και της αποκρυπτογράφησης και η μείωση κατανάλωσης της υπολογιστικής ισχύς που απαιτείται.

Χαρακτηριστικά παραδείγματα αλγόριθμων συμμετρικής κρυπτογραφίας είναι:

- DES - Data Encryption Standard (Αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών).
- Triple DES
- IDEA - International Data Encryption Algorithm
- RC2, RC4, RC5, RC6
- AES - Advanced Encryption Standard

2.3.2. Μη συμμετρική Κρυπτογράφηση - Ασύμμετρη Κρυπτογραφία

Η **μη συμμετρική κρυπτογραφία** ή **κρυπτογραφία δημοσίου κλειδιού (Public Key Cryptography)**[9] αποτελεί μία επινόηση των Whitfield Diffie και Martin Hellman, στα τέλη της δεκαετίας του 1970. Αντιθέτως με τη συμμετρική κρυπτογραφία, στην μέθοδο αυτή στη οποία γίνεται χρήση διαφορετικών κλειδιών για διαφορετικές λειτουργίες τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση.

Ο κάθε χρήστης έχει στη διάθεσή του δύο διαφορετικά κλειδιά κρυπτογράφησης: το ιδιωτικό κλειδί (private key) και το δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει να προφυλάσσεται και να διατηρείται κρυφό από τον κάθε χρήστη, ενώ αντιθέτως το δημόσιο κλειδί θα μπορεί να είναι διαθέσιμο και να χρησιμοποιείται από τον οποιονδήποτε.

Το ιδιωτικό και το δημόσιο κλειδί έχουν εξάρτηση μαθηματική σχέσης μεταξύ τους. Δηλαδή, εφόσον το πρώτο χρησιμοποιηθεί για την κρυπτογράφηση ενός μηνύματος, το δεύτερο θα χρησιμοποιηθεί για την αποκρυπτογράφηση αυτού. Αυτό συνεπάγεται ότι δεν είναι δυνατόν γνωρίζοντας κάποιος ένα δημόσιο κλειδί κρυπτογράφησης, να μπορεί να υπολογίσει ποιο θα είναι το ιδιωτικό κλειδί της κρυπτογράφησης. Συνεπώς, η βασική δυσκολία η οποία υπήρχε στη συμμετρική κρυπτογραφία ξεπερνιέται.

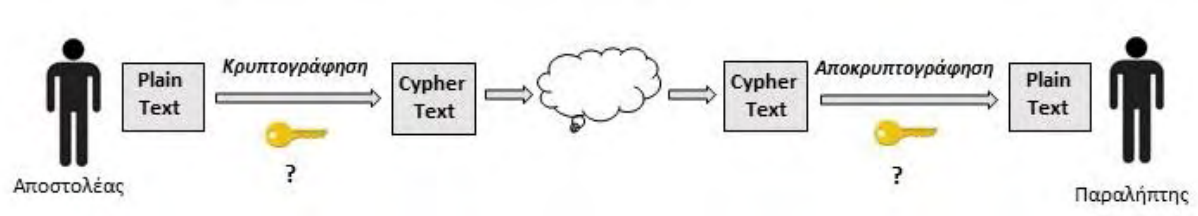
Στη συνέχεια, θα αναλύσουμε δύο παραδείγματα χρήσης αλγορίθμων δημοσίου κλειδιού. Έστω οι χρήστες Α και Β, έκαστος εκ των οποίων διαθέτει ένα δημόσιο κι ένα ιδιωτικό κλειδί Α (PUA, PRA), όπου PUA το δημόσιο κλειδί (public) του Α και PRA το ιδιωτικό κλειδί (private) του Α και αντίστοιχα Β (PUB, PRB), όπου PUB το δημόσιο κλειδί (public) του Α και PRB το ιδιωτικό κλειδί (private) του Α.

- **<u>Παράδειγμα 1ο – Εξασφάλιση Εμπιστευτικότητας</u>**

Πώς με χρήση κρυπτογραφικού αλγορίθμου δημοσίου κλειδιού μπορούμε να εγγυηθούμε ότι το κρυπτογραφημένο μήνυμα που θα αποσταλεί διαδικτυακά από τον αποστολέα (έστω τον Α) στον παραλήπτη θα μπορεί να το αναγνωστεί από αυτόν και μόνο (εμπιστευτικότητα - confidentiality);

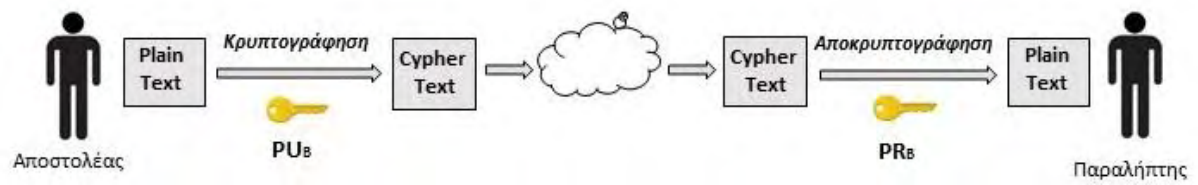
[9] http://www.garykessler.net/library/crypto.html#skc

Ή θέτοντάς το αλλιώς, ποιο θα είναι το κλειδί το οποίο θα χρησιμοποιήσει ο αποστολέας κατά την κρυπτογράφηση;



Εικόνα 4: Εξασφάλιση εμπιστευτικότητας (1)

Το δημόσιο κλειδί του παραλήπτη θα χρησιμοποιηθεί από τον αποστολέα για την κρυπτογράφηση του μηνύματος. Στη συνέχεια, ο παραλήπτης θα χρησιμοποιήσει το ιδιωτικό του κλειδί για την αποκρυπτογράφηση του μηνύματος.



Εικόνα 5: Εξασφάλιση εμπιστευτικότητας (2)

Ο παραλήπτης προχωρά στην αποκρυπτογράφηση του μηνύματος εφόσον το ιδιωτικό του κλειδί είναι γνωστό μόνο στον ίδιο και όχι σε κάποιον άλλο.

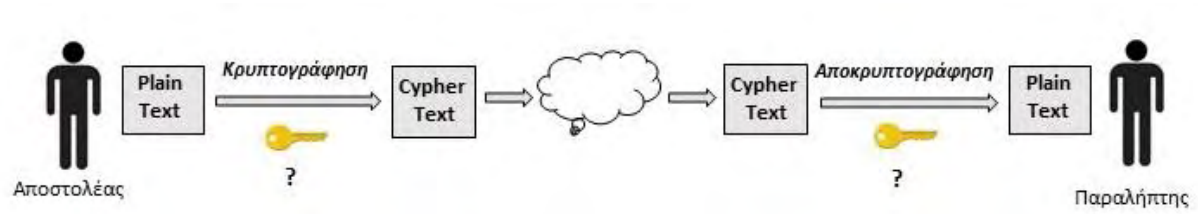
Συνεπώς, διασφαλίζεται η εμπιστευτικότητα του μηνύματος, εφόσον ο αποστολέας γνωρίζει ότι μόνο ο παραλήπτης έχει τη δυνατότητα της αποκρυπτογράφησης του κρυπτογραφημένου μηνύματος.

- **<u>Παράδειγμα 2ο – Εξασφάλιση Πιστοποίησης Αποστολέα</u>**

Με την παραπάνω μέθοδο εξασφαλίσαμε μόνο την εμπιστευτικότητα του αποστολέα και όχι την πιστοποίηση του αποστολέα, δηλαδή την εγγύηση της ταυτότητάς του.

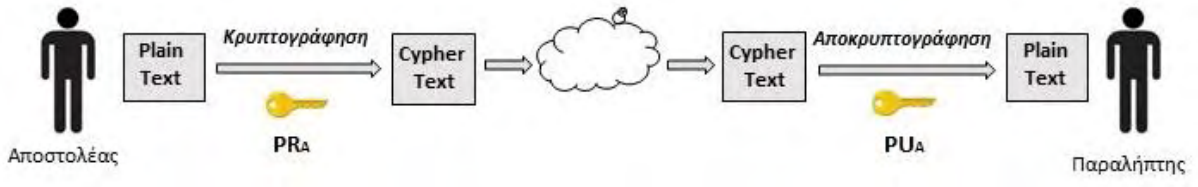
Το ερώτημα που τίθεται είναι πως μπορεί ο παραλήπτης να είναι σίγουρος ποιος είναι ο αποστολέας, δηλαδή να υπάρχει πιστοποίηση (authentication); Ή, όπως και παραπάνω, ποιο

θα είναι το κλειδί το οποίο θα χρησιμοποιηθεί από το αποστολέα κατά την διαδικασία της κρυπτογράφησης;



Εικόνα 6: Πιστοποίηση ταυτότητας αποστολέα (1)

Το ιδιωτικό του κλειδί του αποστολέα χρησιμοποιείται από τον παραλήπτη για την κρυπτογράφηση του μηνύματος. Στην συνέχεια το δημόσιο κλειδί του αποστολέα χρησιμοποιείται από τον παραλήπτη για την αποκρυπτογράφησή του.



Εικόνα 7: Πιστοποίηση ταυτότητας αποστολέα (2)

Ο παραλήπτης μπορεί να επιβεβαιώσει την ταυτότητα του αποστολέα, εφόσον ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονό σε αυτόν. Βέβαια η παραπάνω μέθοδος όπως αναφέραμε, πιστοποιεί μόνο την ταυτοποίηση του αποστολέα, και όχι την εμπιστευτικότητα του μηνύματος. Συνεπώς, η αποκρυπτογράφηση του μηνύματος μπορεί να γίνει από όποιον έχει στη διάθεσή του δημόσιο κλειδί του αποστολέα.

- **<u>Παράδειγμα 3ο - Εξασφάλιση Εμπιστευτικότητας και Πιστοποίησης</u>**

Με τον συνδυασμό των δύο παραπάνω τεχνικών όπως παρουσιάστηκαν στα παραδείγματα 1 και 2 μπορούμε να επιτύχουμε και εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Αφενός μεν το κρυπτογραφημένο μήνυμα που θα αποσταλεί διαδικτυακά θα είναι γνωστό στον αποστολέα και στον παραλήπτη και αφετέρου δε ο παραλήπτης να μπορεί να επιβεβαιώσει την ταυτότητα του αποστολέα.

Για να γίνει αυτό, θα πρέπει πρώτα το μήνυμα να κρυπτογραφηθεί με το ιδιωτικό κλειδί του αποστολέα και έπειτα με το δημόσιο κλειδί του παραλήπτη. Όταν το μήνυμα ληφθεί από τον παραλήπτη, θα πρέπει να χρησιμοποιηθεί το ιδιωτικό του κλειδί για να επιτευχθεί η αποκρυπτογράφηση (εμπιστευτικότητα) και ακολούθως, να γίνει η αποκρυπτογράφηση του αποτελέσματος με την χρήση του δημόσιου κλειδιού του αποστολέα (πιστοποίηση).

2.3.3. Τριμερής Ασύμμετρη Κρυπτογραφία

Η τριμερής ασύμμετρη κρυπτογραφία έρχεται να διορθώσει το κύριο μειονέκτημα της ασύμμετρης κρυπτογραφίας, το οποίο είναι η αβεβαιότητα σε σχέση με την αυθεντικότητα ή μη του δημόσιου κλειδιού, δηλαδή το κατά πόσο το μήνυμα που λαμβάνει ο παραλήπτης προέρχεται από τον αποστολέα/υπογράφων και όχι από κάποιον που παριστάνει τον αποστολέα. Θεωρήθηκε λοιπόν αναγκαίο να υπάρξει ένας τρίτος φορέας ο οποίος και θα αναλάμβανε το έργο της πιστοποίησης και της εγγύησης ότι το δημόσιο κλειδί που χρησιμοποιήθηκε για την αποκρυπτογράφηση ενός ηλεκτρονικού μηνύματος ανήκει πραγματικά στον νόμιμο κάτοχό του.

Ο φορέας αυτός είναι η ενδιάμεση τρίτη έμπιστη οντότητα και ονομάζεται **Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ)**. Ορίζεται ως «***το φυσικό ή νομικό πρόσωπο ή και άλλος φορέας που εκδίδει πιστοποιητικά ή παρέχει υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές»***, σύμφωνα με το άρθρο 2 του Π.Δ. 150/2001.

Έτσι, μέσω της διμερούς συμβατικής σχέσης μεταξύ του ΠΥΠ και του νόμιμου κατόχου του δημόσιου κλειδιού, πραγματοποιείται η πιστοποίηση της μοναδικής σχέση του δημοσίου κλειδιού με τον κάτοχό του και επιβεβαιώνεται μια από τις σημαντικότερες λειτουργίες του ΠΥΠ. Με αυτόν τρόπο, εγγυώνται τα στοιχεία του κατόχου του και ταυτόχρονα εξαλείφεται κάθε πιθανή υποψίας εξαπάτησης. Η ταυτοποίηση αυτού που υπογράφει το ηλεκτρονικό μήνυμα με αυτόν που είναι νόμιμος κάτοχος του δημοσίου κλειδιού αποκρυπτογράφησης του μηνύματος, γίνεται όπως προαναφέρθηκε μέσω του δημοσίου κλειδιού του ΠΥΠ. Ο ΠΥΠ, στο ενδιάμεσο, χρησιμοποιώντας το δικό του ιδιωτικό κλειδί, έχει υπογράψει και επικυρώσει τα δημόσια κλειδιά των νόμιμων κατόχων των ηλεκτρονικών υπογραφών.

2.3.4. Λογισμικό Κρυπτογράφησης PGP (Pretty Good Privacy)

Για την διαδικασία της κρυπτογράφησης είναι απαραίτητη η ύπαρξη ενός λογισμικού. Το λογισμικό που θα περιγράψουμε στην ενότητα αυτή είναι το λογισμικό Pretty Good Privacy (PGP)[10]. Είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας και σχεδιάστηκε από τον Phill Zimmerman το 1999. Η κύρια χρήση του PGP περιλαμβάνει την ψηφιακή υπογραφή, την κρυπτογράφηση και την αποκρυπτογράφηση κειμένων και την ασφαλή επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου. Τα πλεονεκτήματά του είναι ότι δύναται να:

- Διασφαλίζει το απόρρητο κατά την ανταλλαγή αρχείων,
- Πιστοποιεί την ταυτότητα του ατόμου - αποστολέα των μηνυμάτων,
- Παρέχει ευκολία κατά την διαδικασία διασφάλισης του απορρήτου και της πιστοποίησης, ενσωματώνοντας την τεχνολογία της κρυπτογράφησης δημοσίου κλειδιού (public key).
- Επιταχύνει την εκτέλεση των λειτουργιών των δημοσίων κλειδιών σε σχέση με άλλα αντίστοιχα λογισμικά.
- Εξασφαλίζει εργονομικό σχεδιασμό και ποιότητα στην διαχείριση των δημοσίων κλειδιών.

2.4. ΣΤΑΔΙΑ ΔΗΜΙΟΥΡΓΙΑΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ

Αναλύοντας τα παραπάνω, συμπεραίνουμε ότι η ηλεκτρονική υπογραφή χρησιμοποιεί την κρυπτογραφία δημοσίου κλειδιού και βασίζεται στην τεχνολογία της τριμερούς ασύμμετρης κρυπτογραφίας. Ο κάθε χρήστης έχει στη διάθεσή του δύο διαφορετικά κλειδιά κρυπτογράφησης: το ιδιωτικό κλειδί (private key) και το δημόσιο κλειδί (public key). Το ένα κλειδί το χρησιμοποιεί για τη δημιουργία της υπογραφής και το άλλο το χρησιμοποιεί για την επαλήθευσή της.

Η ηλεκτρονική υπογραφή βασίζεται εν μέρει στο δεύτερο παράδειγμα που αναφέραμε και παραπάνω. Το ιδιωτικό του κλειδί του αποστολέα χρησιμοποιείται από τον παραλήπτη για την δημιουργία της. Στην συνέχεια, το δημόσιο κλειδί του αποστολέα χρησιμοποιείται από τον παραλήπτη για την επαλήθευση της.

[10] https://en.wikipedia.org/wiki/Pretty_Good_Privacy

Κατά την διαδικασία δημιουργίας και επαλήθευσης της υπογραφής συμμετέχει και μία μαθηματική συνάρτηση, η **συνάρτηση κατατεμαχισμού** ή **συνάρτηση κατακερματισμού (hash function)**[11]. Η συνάρτηση κατακερματισμού εφαρμόζεται σε ένα μήνυμα ανεξαρτήτου μεγέθους από το οποίο παράγεται η σύνοψή του (**fingerprint** ή **message digest**). Η σύνοψη αυτή αποτελείται από μία σειρά από bits σταθερού μεγέθους (π.χ. από 32 bit μέχρι 256 bits) και είναι μία μοναδική ψηφιακή αναπαράσταση του μηνύματος το οποίο αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού έχει σχεδιαστεί με τέτοιο τρόπο ώστε να είναι μονόδρομη, δηλαδή να είναι δύσκολο να αντιστραφεί η διαδικασία της. Από τη σύνοψη που δημιουργείται, είναι πρακτικά αδύνατον να εξαχθεί το αρχικό μήνυμα. Επίσης, είναι πολύ μικρή η πιθανότητα η σύνοψη δύο μηνυμάτων να είναι ίδια. Δηλαδή, αν χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού, το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης έχει διαφορετική σύνοψη, τότε έχει υποστεί αλλοίωση το μήνυμα κατά την μετάδοσή του (δεν παραδόθηκε ακέραιο). Η διαφοροποίηση ενός μηνύματος θα επιφέρει και τη διαφοροποίηση της σύνοψης.

Παρακάτω περιγράφονται αναλυτικά τα στάδια δημιουργίας και επαλήθευσης μιας ηλεκτρονικής - ψηφιακής υπογραφής.

1. Δημιουργία ηλεκτρονικής υπογραφής

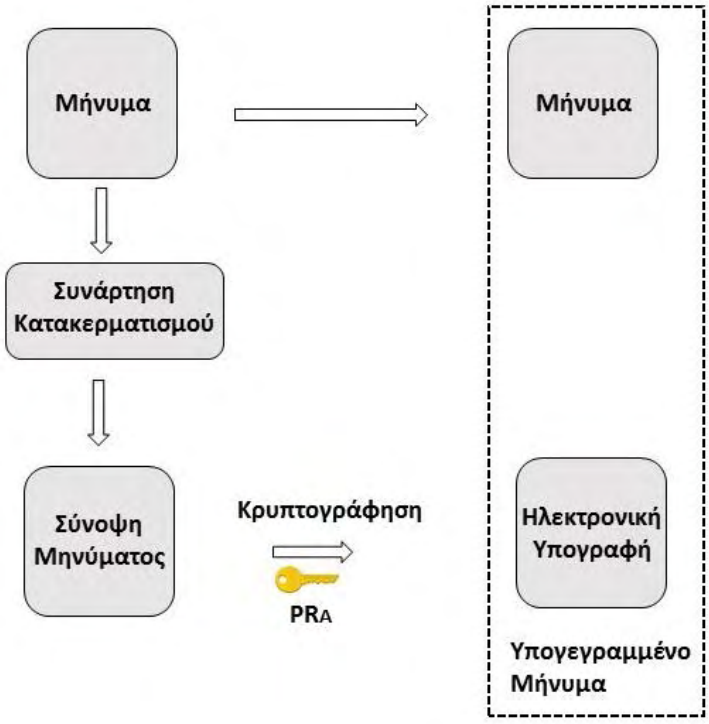
Αποστολέας

- Ο αποστολέας χρησιμοποιεί την συνάρτηση (αλγόριθμο) κατακερματισμού και δημιουργεί τη σύνοψη του μηνύματος που θέλει να αποστείλει. Παράγεται λοιπόν μία σειρά ψηφίων συγκεκριμένου μήκους, ανεξάρτητα από το μέγεθος του μηνύματος.
- Ο αποστολέας χρησιμοποιώντας το ιδιωτικό του κλειδί, κρυπτογραφεί τη σύνοψη του μηνύματος.
- Η κρυπτογραφημένη σύνοψη με το ιδιωτικό κλειδί του αποστολέα είναι ουσιαστικά η ηλεκτρονική υπογραφή, δηλαδή μία σειρά ψηφίων συγκεκριμένου πλήθους.

[11] https://en.wikipedia.org/wiki/Hash_function

- Η κρυπτογραφημένη σύνοψη (ηλεκτρονική υπογραφή) που δημιουργείται, προσαρτάται στο αρχικό μήνυμα και το μήνυμα μαζί με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου. Ο αποστολέας έχει τη δυνατότητα να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη.

Η διαδικασία της δημιουργίας της ηλεκτρονικής υπογραφής παρουσιάζεται στην επόμενη εικόνα:



Εικόνα 8: Διαδικασία δημιουργίας ηλεκτρονικής υπογραφής

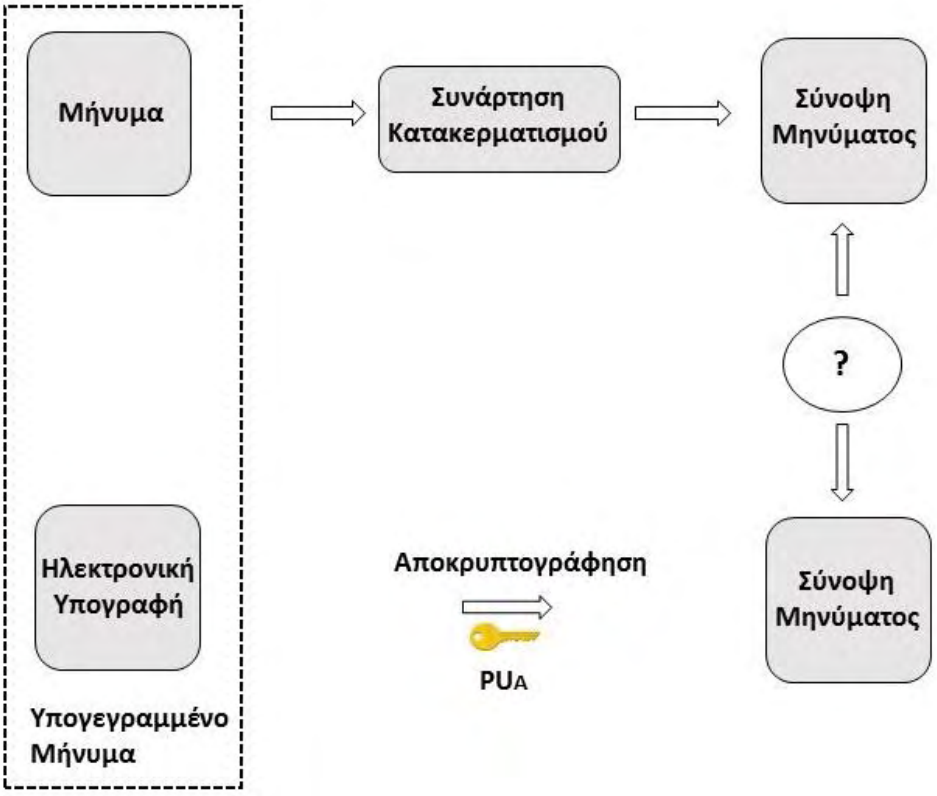
2. Επαλήθευση ψηφιακής υπογραφής

Παραλήπτης

- Η ψηφιακή υπογραφή αποσπάται από το μήνυμα από τον παραλήπτη.
- Ο παραλήπτης εφαρμόζει στο μήνυμα που απέσπασε την ίδια συνάρτηση (αλγόριθμο) κατακερματισμού και έτσι δημιουργείται η δική του σύνοψη του μηνύματος.

- Κατόπιν, αποκρυπτογραφείται η ψηφιακή υπογραφή (κρυπτογραφημένη σύνοψη του μηνύματος) με το δημόσιο κλειδί του αποστολέα.
- Τέλος, γίνεται σύγκριση και των δύο συνόψεων και αν ταιριάζουν, αυτό σημαίνει ότι το μήνυμα το οποίο έλαβε ο παραλήπτης είναι αυθεντικό και ακέραιο. Εάν υπάρχει τροποποίηση του μηνύματος, τότε η σύνοψη που θα παράγει ο παραλήπτης δεν θα είναι ίδια με την σύνοψη που έχει κρυπτογραφηθεί.

Η διαδικασία επαλήθευσης της ηλεκτρονικής υπογραφής παρουσιάζεται στην επόμενη εικόνα:



Εικόνα 9: Διαδικασία επαλήθευσης ηλεκτρονικής υπογραφής

Είναι ευνόητο ότι οι παραπάνω διαδικασίες πραγματοποιούνται από ανάλογο λογισμικό εγκατεστημένο στον υπολογιστή του χρήστη και δεν απαιτεί την μεσολάβηση του χρήστη για την δημιουργία και έλεγχο των δύο συνόψεων. Ο χρήστης δεν είναι υποχρεωμένος να γνωρίζει εξειδικευμένες τεχνικές λεπτομέρειες ώστε να μπορεί να υπογράφει ψηφιακά.

Παρατηρώντας τις ανωτέρω διαδικασίες, διαπιστώνουμε ότι η ηλεκτρονική υπογραφή εξαρτάται αποκλειστικά από: α) τον υπογράφοντα, μέσω του ιδιωτικού του κλειδιού και β) το ίδιο το κείμενο (μήνυμα), μέσω της σύνοψης του. Συνεπώς, αντιθέτως με την ιδιόχειρη

υπογραφή, η ηλεκτρονική υπογραφή ενός ίδιου ατόμου είναι διαφορετική από μήνυμα σε μήνυμα.

2.5. ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ - ΨΗΦΙΑΚΟ ΠΙΣΤΟΠΟΙΗΤΙΚΟ

Κατά την παραλαβή ενός μηνύματος που έχει υπογραφεί ψηφιακά, ο παραλήπτης επιβεβαιώνει την ακεραιότητα του μηνύματος μέσω της επαλήθευσης της ηλεκτρονικής υπογραφής. Ο παραλήπτης, για να επαληθεύσει την ηλεκτρονική υπογραφή, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Από την άλλη μεριά, ο παραλήπτης δεν μπορεί να γνωρίζει με σιγουριά εάν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Για αυτό τον λόγο, χρειάζεται να υπάρχει μία διαδικασία έτσι ώστε ο παραλήπτης να είναι σε θέση να γνωρίζει την ταυτότητα του προσώπου που έχει το δημόσιο κλειδί. Θα πρέπει να εξασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού είναι αυτός που δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιείται από τον παραλήπτη για την επαλήθευση της υπογραφής είναι όντως του αποστολέα.

Η παραπάνω διαδικασία θα πρέπει να υλοποιηθεί από μία τρίτη οντότητα εμπιστοσύνης, η οποία εγγυάται ότι το συγκεκριμένο δημόσιο κλειδί αντιστοιχεί και στο συγκεκριμένο πρόσωπο. Αυτή η οντότητα ονομάζεται Πάροχος Υπηρεσιών Πιστοποίησης (όπως έχει αναφερθεί και παραπάνω) και είναι η υπηρεσία εκείνη η οποία πιστοποιεί την σχέση ενός προσώπου με το δημόσιο κλειδί του. Σε συνέχεια του σκοπού αυτού, **εκδίδεται ένα πιστοποιητικό (ηλεκτρονικό αρχείο), στο οποίο ο πάροχος υπηρεσιών πιστοποίησης πιστοποιεί αφενός την ταυτότητα του προσώπου και αφετέρου το δημόσιο κλειδί του.**

Το πιστοποιητικό είναι γνωστό με το όνομα **πιστοποιητικό δημόσιου κλειδιού (public key certificate**) ή αλλιώς **ψηφιακό πιστοποιητικό**[12] ή **πιστοποιητικό ταυτότητας**. Είναι στην ουσία ένα ηλεκτρονικό έγγραφο απόδειξης της κυριότητας ενός δημοσίου κλειδιού.

Για την έκδοση ενός ψηφιακού πιστοποιητικού, θα πρέπει ο ενδιαφερόμενος να υποβάλλει αίτηση σε μία Αρχή Πιστοποίησης. Στην συνέχεια, επιβεβαιώνεται η ταυτότητα του αιτούντος

[12] https://en.wikipedia.org/wiki/Public_key_certificate

από την Αρχή Πιστοποίησης και εκδίδεται το πιστοποιητικό, το οποίο και περιλαμβάνει τα παρακάτω βασικά στοιχεία:

- Πληροφορίες που αφορούν τον κάτοχο του πιστοποιητικού (Όνομα, Επώνυμο, e-mail κ.α.).
- Το όνομα της Αρχής Πιστοποίησης που εξέδωσε το πιστοποιητικό.
- Την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που εξέδωσε το πιστοποιητικό.
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού.
- Το χρονικό διάστημα εγκυρότητας του πιστοποιητικού.

Τα ψηφιακά πιστοποιητικά χωρίζονται σε δύο μεγάλες κατηγορίες:

1. Πιστοποιητικά χαλαρής αποθήκευσης, που είναι ψηφιακά πιστοποιητικά εγκατάστασης στον υπολογιστή του τελικού χρήστη. **Τα πιστοποιητικά αυτά ονομάζονται ψηφιακά πιστοποιητικά τύπου Β (class B) και μπορούν να αντιγραφούν σε άλλο μέσο.**
2. Πιστοποιητικά σκληρής αποθήκευσης, που είναι ψηφιακά πιστοποιητικά αποθήκευσης σε ΑΔΔΥ (Ασφαλή Διάταξη Δημιουργίας Υπογραφής). Η ΑΔΔΥ μπορεί να είναι μία έξυπνη κάρτα - smartcard ή ένα USB token και αναλύονται παρακάτω. **Τα πιστοποιητικά αυτά ονομάζονται ψηφιακά πιστοποιητικά τύπου Α (class A) και δεν μπορούν να αντιγραφούν σε άλλο μέσο.**

2.6. ΑΣΦΑΛΗΣ ΔΙΑΤΑΞΗ ΔΗΜΙΟΥΡΓΙΑΣ ΥΠΟΓΡΑΦΗΣ (ΑΔΔΥ)

2.6.1. Έξυπνη Κάρτα (Smart Card)

Η Έξυπνη κάρτα (Smart card)[13] είναι μια κάρτα, η οποία εξωτερικά εμφανίζει πολλές ομοιότητες με την πιστωτική κάρτα. Η διαφορά της όμως είναι ότι στην έξυπνη κάρτα, ενσωματώνεται ένας μικροεπεξεργαστής, κάτω από μια επαφή από χρυσό, εκεί όπου και γίνεται η αποθήκευση των δεδομένων.

[13] https://en.wikipedia.org/wiki/Smart_card

Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν επιτραπεί η πρόσβαση στα δεδομένα της μνήμης της κάρτας. Έτσι αποφεύγεται η αλλοίωση και παραχάραξη των δεδομένων, ούτως ώστε σε περίπτωση που η κάρτα του χρήστη χαθεί από τα δικά του χέρια, ο χρήστης να είναι διασφαλισμένος.

Τεχνικά Χαρακτηριστικά Έξυπνης Κάρτας:

- Το μέγεθος μνήμης RAM είναι μέχρι 8 Kbytes,
- Το μέγεθος μνήμης ROM είναι μέχρι 346 Kbytes,
- Το μέγεθος μνήμης PROM (προγραμματιζόμενη ROM) είναι μέχρι 256kbytes,
- Το μέγεθος Μικροεπεξεργαστή είναι συνήθως 16 bytes.

Παρακάτω παρουσιάζονται οι όψεις από μία έξυπνη κάρτα - ακαδημαϊκή ταυτότητα[14]:

Εικόνα 10: Εμπρόσθια όψη έξυπνης κάρτας

[14]https://academicid.minedu.gov.gr. Η ταυτότητα αυτή χορηγείται σε καθηγητές και προσωπικό των Ακαδημαϊκών Ιδρυμάτων της χώρας από το ακαδημαϊκό έτος 2014-15.

Εικόνα 11: Οπίσθια όψη έξυπνης κάρτας

<u>Αναγνώστης Έξυπνης Κάρτας (Smart Card Reader)</u>

Προκειμένου να χρησιμοποιηθεί μία έξυπνη κάρτα, θα πρέπει να συνοδεύεται από τον αναγνώστη έξυπνης κάρτας (smart card reader),ο οποίος παρέχει της τροφοδοσία της κάρτας με ενέργεια.

Ο αναγνώστης αναλαμβάνει την επικοινωνία με κάποιο κεντρικό υπολογιστή, όπου έχουν αποθηκευτεί τα στοιχεία του χρήστη και εξασφαλίζει την πρόσβαση σε δεδομένα. Παρακάτω παρουσιάζονται οι όψεις από έναν αναγνώστη έξυπνης κάρτας:

Εικόνα 12: Εμπρόσθια όψη αναγνώστη έξυπνης κάρτας

Εικόνα 13: Οπίσθια όψη αναγνώστη έξυπνης κάρτας

2.6.2. USB Token

Το USB token[15] είναι μία ηλεκτρονική συσκευή που έχει πολλές εξωτερικές ομοιότητες με την μνήμη USB Flash. Είναι μία ειδική συσκευή που συνδέεται σε θύρα USB του υπολογιστή και η οποία λειτουργεί ως ασφαλής χώρος αποθήκευσης ψηφιακών πιστοποιητικών. Έχει παρόμοια τεχνικά χαρακτηριστικά με την έξυπνη κάρτα και χρησιμοποιείται για την δημιουργία ψηφιακής υπογραφής. Παρακάτω παρουσιάζονται οι όψεις από ένα USB token, τύπου **Safenet 5100**:

Εικόνα 14: Εμπρόσθια όψη USB token, Safenet 5100

[15] https://el.wikipedia.org/wiki/USB_Token

Εικόνα 15: Οπίσθια όψη USB token, Safenet 5100

2.7. ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (ΥΔΚ)

Όπως είδαμε και παραπάνω, κατά την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης βεβαιώνεται για την ακεραιότητα του μηνύματος και για την ταυτότητα του υπογράφοντα επαληθεύοντας την ηλεκτρονική υπογραφή.

Για την επαλήθευση της ηλεκτρονικής υπογραφής, ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Είναι απαραίτητο να εξασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, ο αποστολέας δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του, που χρησιμοποιείται από τον παραλήπτη για την επαλήθευση της υπογραφής, είναι όντως δικό του (του αποστολέα). **Η Υποδομή Δημοσίου Κλειδιού (ΥΔΚ) είναι ο μηχανισμός που χρησιμοποιείται ώστε ο παραλήπτης να επιβεβαιώνει την ταυτότητα του προσώπου που φέρει το δημόσιο κλειδί (αποστολέας).**

Η **Υποδομή Δημόσιου Κλειδιού (ΥΔΚ) / Public Key Infrastructure** (**PKI**) είναι ένα σύνολο λογισμικού, τεχνολογιών κρυπτογράφησης, και υπηρεσιών που πιστοποιούν την εγκυρότητα ενός φυσικού προσώπου σε μια διαδικτυακή συναλλαγή ενώ παράλληλα είναι υπεύθυνη για την ασφάλεια αυτής της συναλλαγής. Στηρίζεται στην ανταλλαγή ψηφιακών πιστοποιητικών μεταξύ εξουσιοδοτημένων χρηστών και δικτυακών τόπων.

Στόχος της Υποδομής Δημόσιου Κλειδιού είναι η εξασφάλιση των παρακάτω προϋποθέσεων:

- Ακεραιότητα δεδομένων (integrity)
- Πιστοποίηση Αυθεντικότητας δεδομένων (authentication).
- Εμπιστευτικότητα δεδομένων (confidentiality)
- Μη Άρνηση Αποδοχής (non-repudiation)

Παρακάτω, παραθέτουμε τους επόμενους ορισμούς, στους οποίους βασίζεται η έννοια της Υποδομής Δημοσίου Κλειδιού.

2.7.1. Ορισμοί και ρόλοι της Υποδομής Δημοσίου Κλειδιού (ΥΔΚ)

• **Ψηφιακό Πιστοποιητικό**. Είναι στην ουσία ένα ηλεκτρονικό έγγραφο απόδειξης της κυριότητας ενός δημοσίου κλειδιού.

• **Αρχή Πιστοποίησης (ΑΠ)** είναι ο πιστοποιημένος Φορέας έκδοσης, χειρισμού, ανανέωσης και ανάκλησης πιστοποιητικών.

• **Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ)** είναι η αρχή που εκδίδει πιστοποιητικά προς τις **Υποκείμενες ΑΠ (ΥπΑΠ)**.

• **Αρχή Εγγραφής (ΑΕ)** είναι ο φορέας υποβοήθησης για την αίτηση πιστοποιητικών και είναι εγκεκριμένος από την ΑΠ.

• Τα **Εντεταλμένα Γραφεία (ΕΕ)** αναφέρονται στην προϊσταμένη Αρχή Εγγραφής και είναι αρμόδια για την διεκπεραίωση όλων αιτημάτων των πιστοποιητικών και την επιβεβαίωση των στοιχείων ταυτότητας των Τελικών Χρηστών.

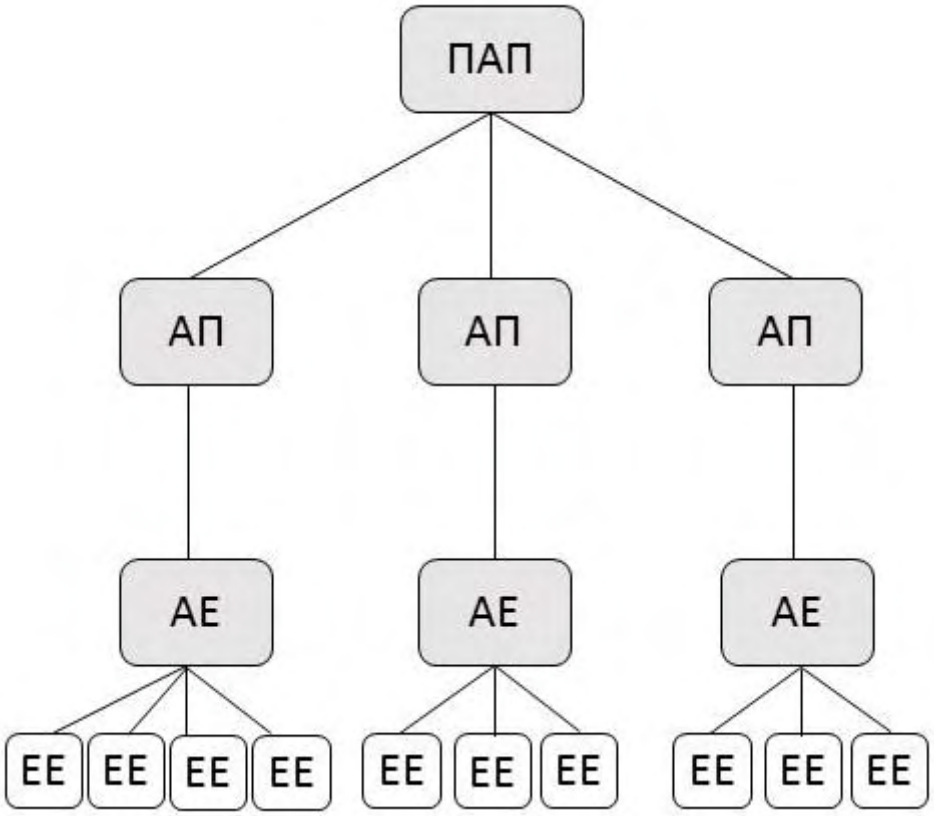
• **Ηλεκτρονική Υπογραφή** είναι ένα σύνολο δεδομένων σε ψηφιακή μορφή που χρησιμοποιούνται για την απόδειξη της αυθεντικότητας και της εγκυρότητας ενός μηνύματος.

• **Προηγμένη ηλεκτρονική υπογραφή** είναι η ηλεκτρονική υπογραφή, που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται με χρήση ασφαλούς μέσου (ειδικό κρυπτογραφικό υλικό - ΑΔΔΥ).

• Ο **Τελικός Χρήστης** είναι αυτός που κατέχει ένα ιδιωτικό κλειδί το οποίο το χρησιμοποιεί για να το αντιστοιχίσει με το δημόσιο κλειδί.

- Ο **Τρίτος Συμμετέχων** είναι ένας φορέας ή φυσικό πρόσωπο που ενεργεί βασιζόμενος σε κάποιο πιστοποιητικό.
- Οι **Όροι Χορήγησης Πιστοποιητικού (ΟΧΠ)** είναι οι όροι στους οποίους βασίζεται ένα φυσικό πρόσωπο και ενεργεί ως Τελικός Χρήστης.
- Οι **Όροι Τρίτου Συμμετέχοντα (ΟΤΣ)** είναι οι όροι στους οποίους βασίζεται ένα φυσικό πρόσωπο και ενεργεί ως Τρίτος Συμμετέχων.
- Ο **Κατάλογος Ανακληθέντων Πιστοποιητικών (ΚΑΠ)** είναι ένας κατάλογος που περιλαμβάνει τα πιστοποιητικά που έχουν ανακληθεί.
- Η **Πολιτική Πιστοποίησης (ΠΠ)** παρέχει υπηρεσίες πιστοποίησης για την έκδοση, χειρισμό, ανανέωση και ανάκληση πιστοποιητικών.
- Ο **Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ**), είναι τρίτη έμπιστη οντότητα που είναι υπεύθυνη για την έκδοση ψηφιακών πιστοποιητικών σε χρήστες και για την εξασφάλιση ότι η ηλεκτρονική υπογραφή ενός χρήστη ανήκει σε αυτόν
- Οι **Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής (ΑΔΔΥ)**, είναι οι έξυπνες κάρτες οι οποίες διανέμονται στους χρήστες και μεταξύ άλλων προστατεύουν το ιδιωτικό κλειδί του πιστοποιητικού υπογραφής, καθώς και την ακεραιότητα των πληροφοριών που υπογράφονται.

Στην παρακάτω εικόνα παρουσιάζεται η αρχιτεκτονική της Υποδομής Δημοσίου Κλειδιού (ΥΔΚ).

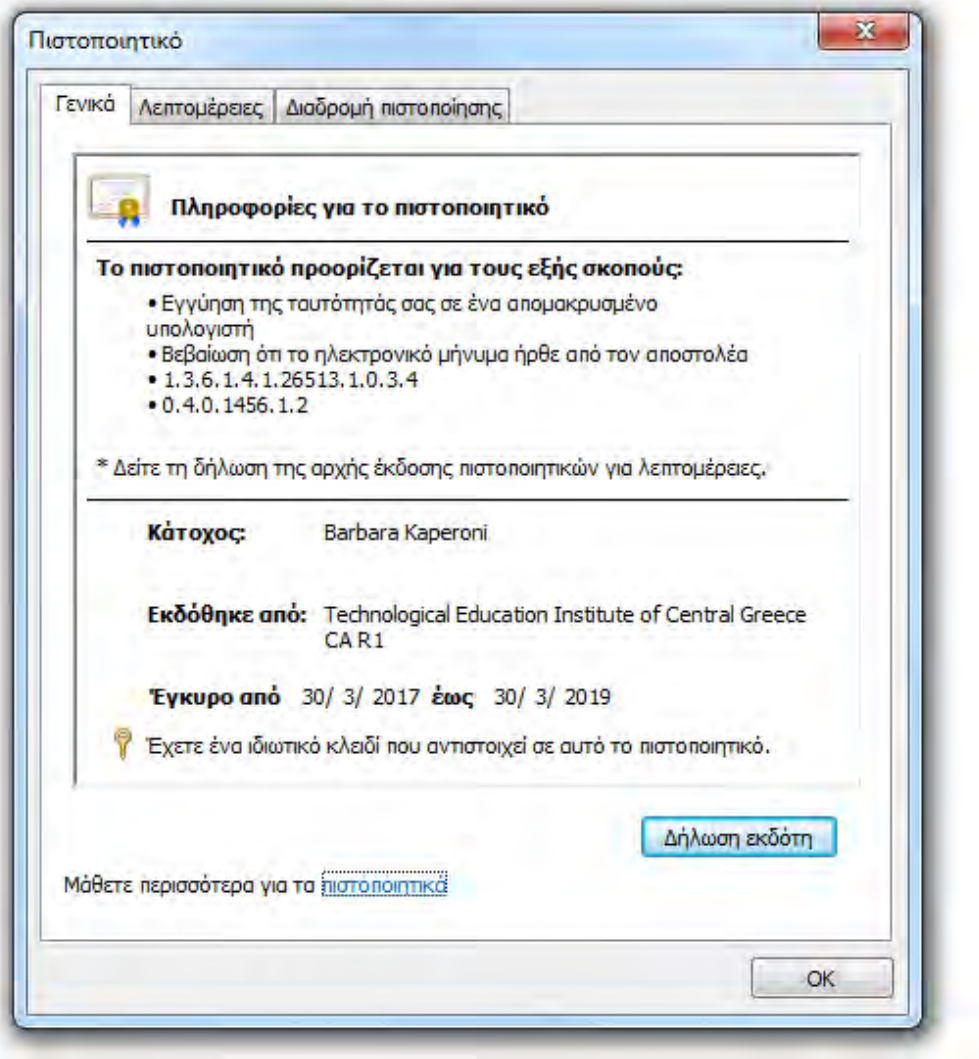


Εικόνα 16: Αρχιτεκτονική PKI

Στη συνέχεια θα δούμε ένα δείγμα πιστοποιητικού χρήστη και πως οι ορισμοί που αναλύσαμε παρουσιάζονται στα χαρακτηριστικά του. Το δείγμα προέκυψε από το άνοιγμα του στο μηχάνημα του χρήστη και από την αποτύπωσή (capture) του.

Στην καρτέλα **Γενικά** του πιστοποιητικού παρέχονται οι παρακάτω πληροφορίες:

- Όνομα Κατόχου
- Φορέας Έκδοσης
- Ημερομηνία εγκυρότητας - Ημερομηνία λήξης (Από - έως)

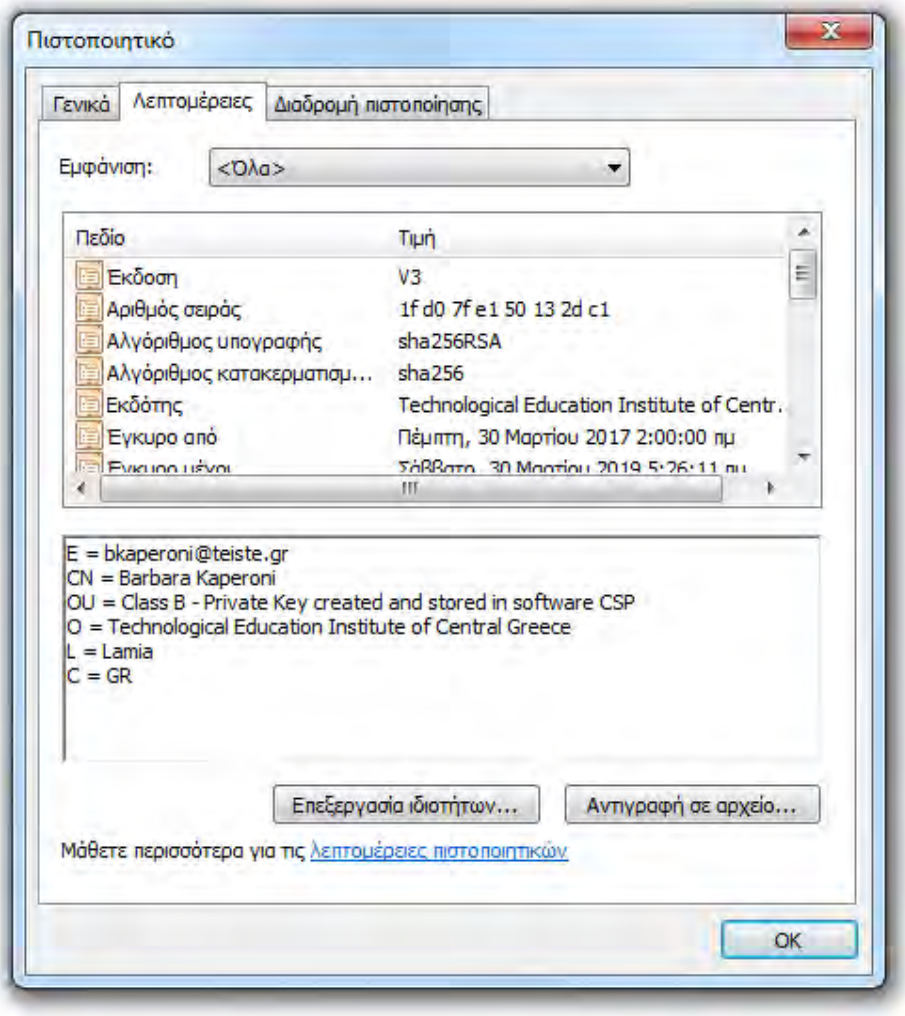


Εικόνα 17: Γενικές πληροφορίες πιστοποιητικού

Στην καρτέλα **Λεπτομέρειες** του πιστοποιητικού παρέχονται οι παρακάτω πληροφορίες:

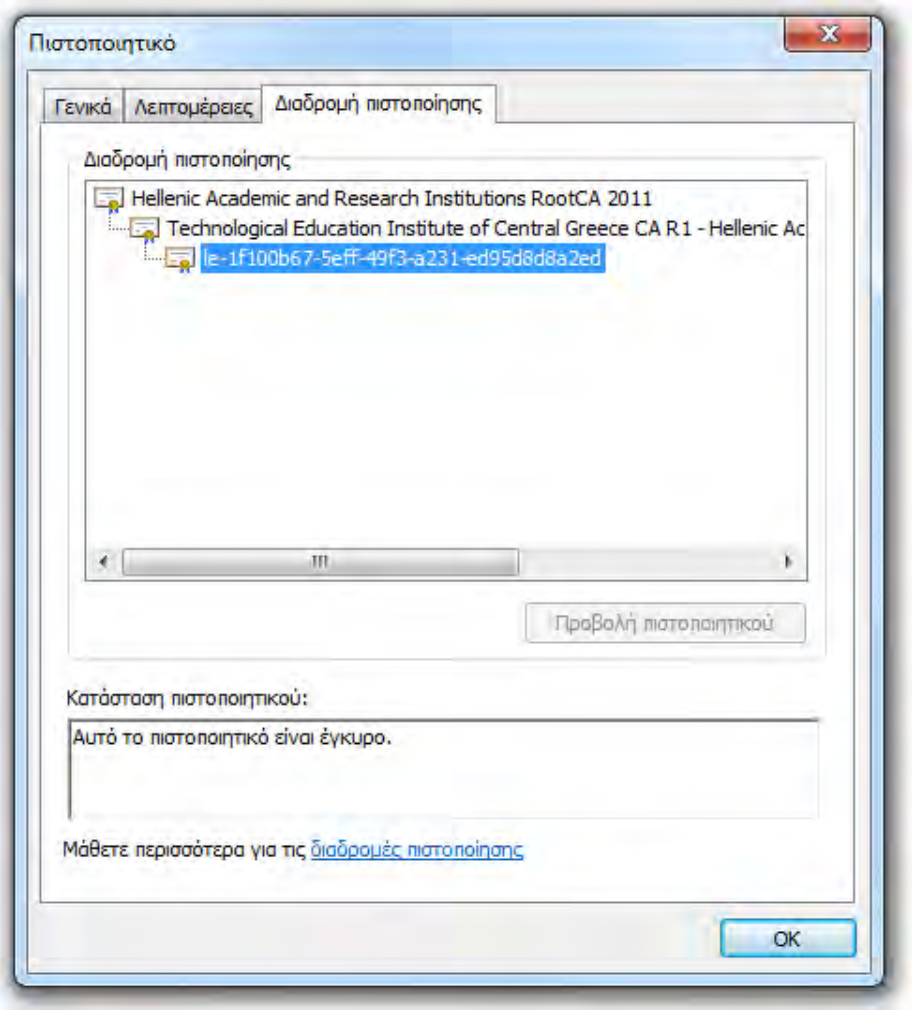
- Country (C) - Χώρα = Όνομα της Χώρας που έχει εκδοθεί (GR)
- (L) = Όνομα της Πόλης που έχει εκδοθεί
- Organization (O) - Οργανισμός = Το Όνομα της Υποκείμενης Αρχής ΑΠ που είναι υπεύθυνη για την έκδοση πιστοποιητικών στους τελικούς χρήστες.
- Organizational Unit (OU) - Οργανική Μονάδα = Ο τύπος και η χρήση του πιστοποιητικού.
- Common Name (CN) - Κοινό Όνομα = Το Ονοματεπώνυμο του τελικού χρήστη.

- E-Mail Address (E) - Ηλεκτρονική Διεύθυνση = Η διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail) του τελικού χρήστη.



Εικόνα 18:Λεπτομέρειες πιστοποιητικού

Στην καρτέλα **Διαδρομή Πιστοποίησης** παρουσιάζεται η ιεραρχία πιστοποίησης και η κατάσταση εγκυρότητας του πιστοποιητικού:



Εικόνα 19: Διαδρομή πιστοποίησης

ΚΕΦΑΛΑΙΟ 3: ΔΙΑΔΙΚΑΣΙΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ ΜΕΣΩ ΤΗΣ HARICA

3.1. ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό θα δούμε πληροφορίες σχετικά με την έμπιστη τρίτη οντότητα την Υποδομή Δημοσίου Κλειδιού (ΥΔΚ) της HARICA. Επίσης, θα περιγράψουμε την διαδικασία έκδοσης ψηφιακής υπογραφής μέσω της HARICA, την διαδικασία ψηφιακής υπογραφής αρχείου και μηνύματος ηλεκτρονικού ταχυδρομείου.

3.2. ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ HARICA

Η Υποδομή Δημοσίου Κλειδιού (ΥΔΚ) της HARICA (Hellenic Academic & Research Institutions Certification Authority) είναι μία κοινή δράση μελών συγκροτημένη από Ακαδημαϊκά Ιδρύματα, Ερευνητικούς φορείς και το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας-ΕΔΕΤ[16]. Αποτελεί μία έμπιστη τρίτη οντότητα που είναι υπεύθυνη για τη πιστοποίηση της ταυτότητας των χρηστών και των δικτυακών εξυπηρετητών όλων των Ακαδημαϊκών Ιδρυμάτων και Ερευνητικών φορέων της Ελλάδας. Η δράση της ξεκίνησε στα πλαίσια χρηματοδοτούμενου έργου από το ΕΔΕΤ μέσω του Επιχειρησιακού προγράμματος «Κοινωνία της Πληροφορίας» και σήμερα φιλοξενείται από το Ακαδημαϊκό Διαδίκτυο (GUnet)[17].

Σκοπός της HARICA είναι η δημιουργία υποδομής με την οποία θα υπάρχει ασφαλής επικοινωνία των μελών που ανήκουν στους Ακαδημαϊκούς και Ερευνητικούς φορείς της Ελλάδας. Είναι υπεύθυνη για:

- Την υλοποίηση Ιεραρχίας Δημοσίου Κλειδιού μέσω της οποίας τα μέλη της (Ακαδημαϊκά Ιδρύματα) αποκτούν ενδιάμεση αρχή Πιστοποίησης, με αρχή την Κεντρική Αρχή Πιστοποίησης της HARICA,
- Την έκδοση ψηφιακών πιστοποιητικών για τα μέλη του,

[16]**Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ ή GRNET):** Δίκτυο παροχής υπηρεσιών Διαδικτύου για την ελληνική πανεπιστημιακή και ερευνητική κοινότητα.
https://en.wikipedia.org/wiki/Greek_Research_and_Technology_Network

[17]**Ακαδημαϊκό Διαδίκτυο (GUnet):** Δίκτυο Ακαδημαϊκών Ιδρυμάτων, https://www.gunet.gr

- Την ασφαλή ανταλλαγή δεδομένων,
- Την απόδειξη της ταυτότητας των μελών του και
- Την ασφαλή επικοινωνία των μελών του μέσω ηλεκτρονικού ταχυδρομείου.

3.3. ΡΥΘΜΙΣΗ ΣΥΣΚΕΥΗΣ ΓΙΑ ΧΡΗΣΗ ΤΗΣ ΕΞΥΠΝΗΣ ΚΑΡΤΑΣ - ΑΚΑΔΗΜΑΪΚΗΣ ΤΑΥΤΟΤΗΤΑΣ

Για την εγκατάσταση και χρησιμοποίηση της ακαδημαϊκής ταυτότητας στον προσωπικό μας υπολογιστή (Λειτουργικό Σύστημα Windows) ακολουθούμε τα παρακάτω βήματα[18]:

Βήμα 1ο :

Πρώτα θα πρέπει να κατεβάσουμε και να εκτελέσουμε το αρχείο Classic Client User setup (32 Bit[19] ή 64 Bit[20] ανάλογα με την έκδοση του λειτουργικού μας συστήματος). Στη συνέχεια, η εκτέλεση θα πρέπει να γίνει ως Διαχειριστής (Administrator). Άρα Δεξί κλικ--> Run as Administrator.

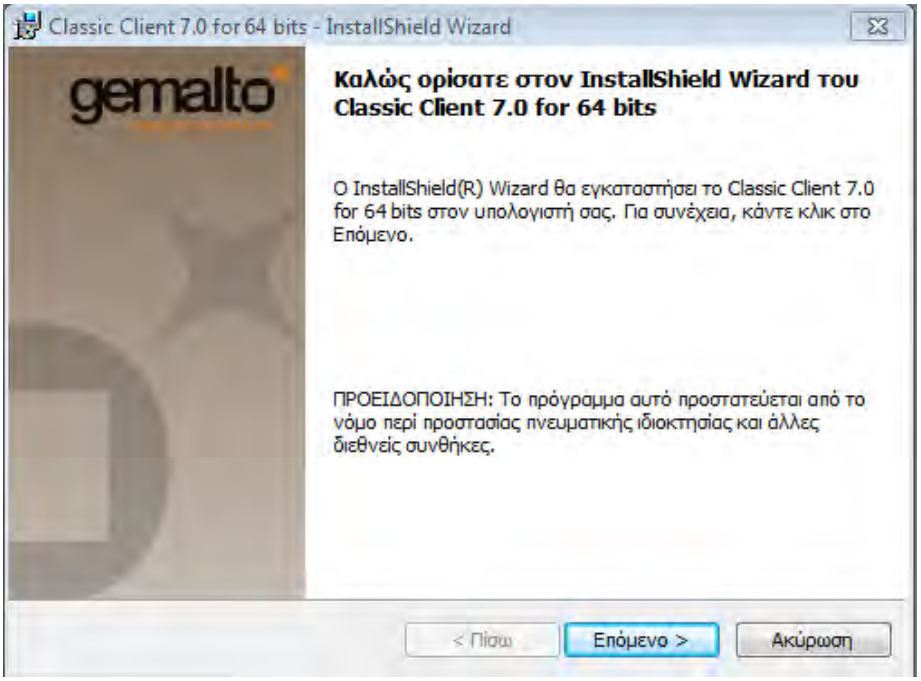
Βήμα 2ο :

Κάνουμε κλικ στο Επόμενο.

[18] https://it.auth.gr/el/setupAcademicId

[19] https://it.auth.gr/sites/default/files/downloads/Classic_Client_32_User_setup.msi

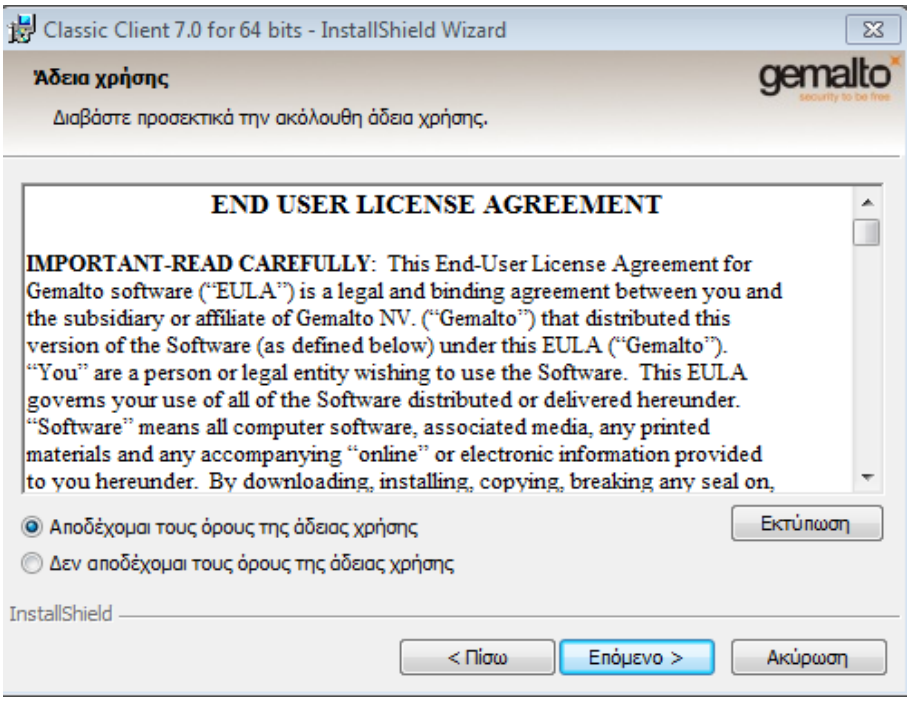
[20] https://it.auth.gr/sites/default/files/downloads/Classic_Client_64_User_setup.msi



Εικόνα 20: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (1)

Βήμα 3ο :

Κάνουμε κλικ στο «Αποδέχομαι τους όρους της άδειας χρήσης» και επιλέγουμε Επόμενο.



Εικόνα 21: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (2)

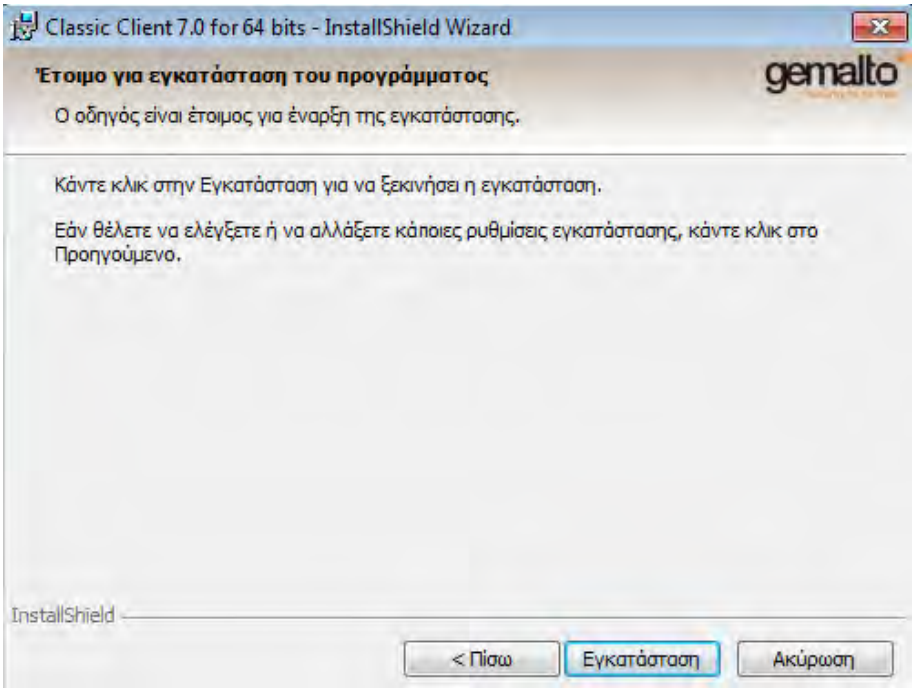
Βήμα 4ο :

Επιλέγουμε και πάλι Επόμενο.

Εικόνα 22: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (3)

Βήμα 5ο :

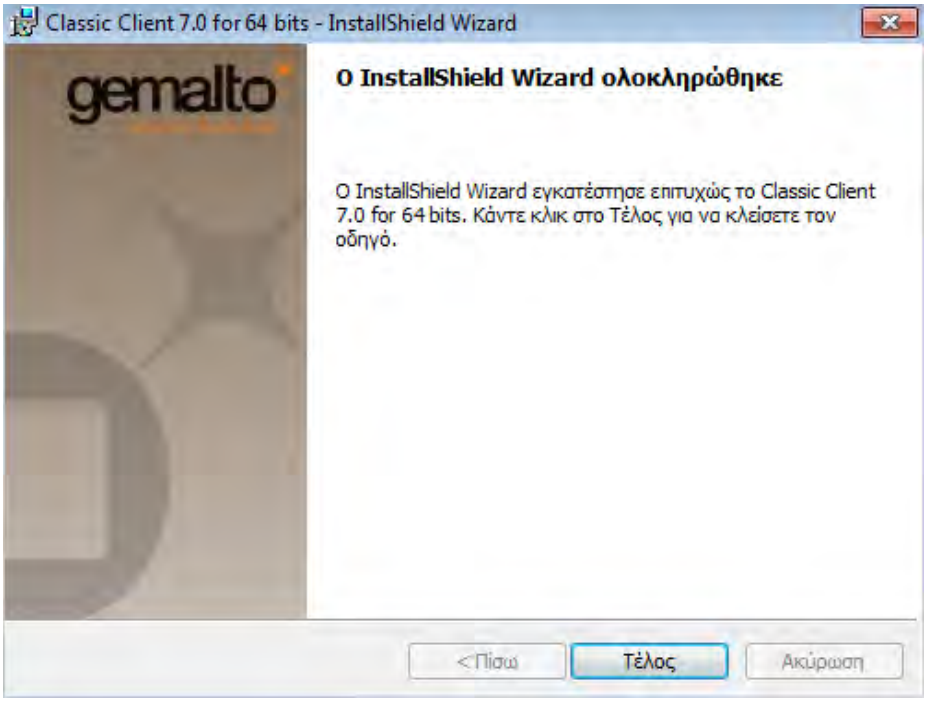
Επιλέγουμε Εγκατάσταση.



Εικόνα 23: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (4)

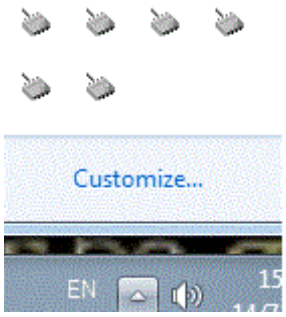
Βήμα 6ο :

Κάνουμε κλικ στο Τέλος.



Εικόνα 24: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (5)

Όταν έχει ήδη ολοκληρωθεί η εγκατάσταση, θα εμφανιστεί το παρακάτω στιγμιότυπο που εμφανίζει πολλά εικονίδια στην γραμμή εργασιών στην μορφή card reader.



Εικόνα 25: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (6)

Βήμα 7ο :

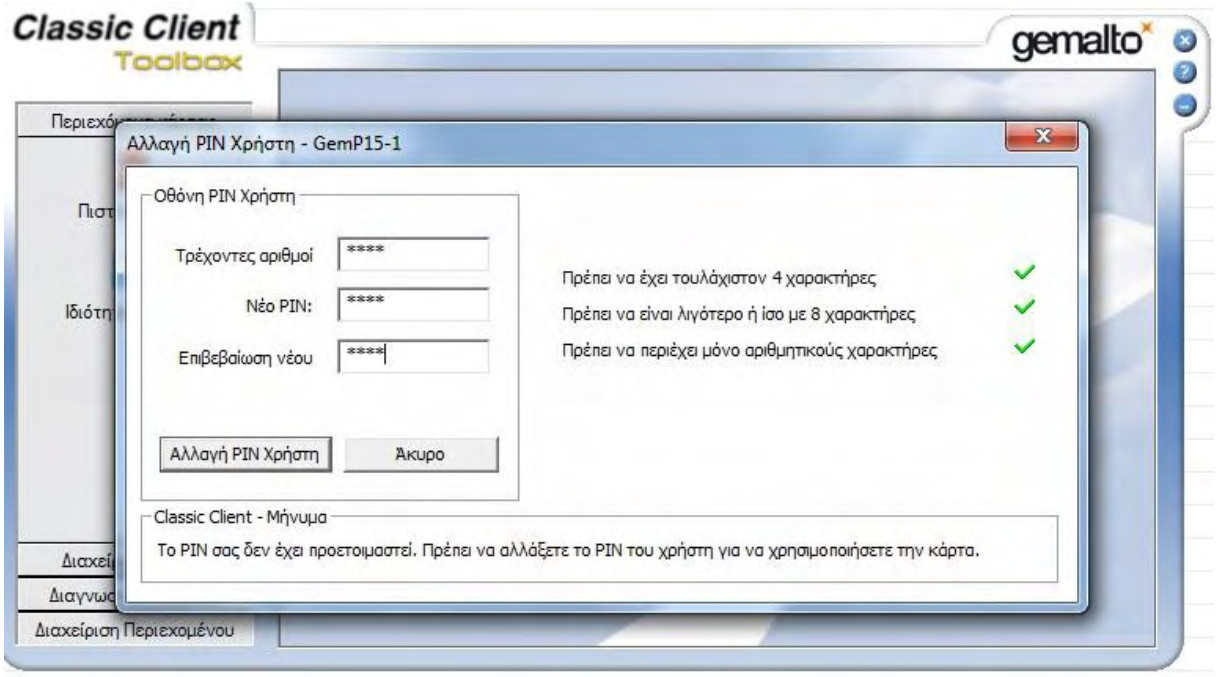
Στην συνέχεια, εισάγουμε τον αναγνώστη της κάρτας (card reader) σε μια USB θύρα του υπολογιστή μας. Στην συνέχεια, εισάγουμε την ακαδημαϊκή μας ταυτότητα (Academic Id) επάνω στον αναγνώστη της κάρτας ώστε να εφαρμόσει κανονικά.

Με το που εισάγουμε την ακαδημαϊκή ταυτότητα, θα παρατηρήσουμε ότι η μορφή σε ένα από τα εικονίδια έχει αλλάξει και συνεπώς είναι έτοιμη για χρήση.

Εικόνα 26: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (7)

Βήμα 8ο :

Μετά την εισαγωγή της ακαδημαϊκής ταυτότητας θα μας ζητηθεί να αλλάξουμε τον προσωπικό κωδικό (PIN) για να μπορέσουμε να χρησιμοποιήσουμε την κάρτα:



Εικόνα 27: Στιγμιότυπο οθόνης εγκατάστασης ακαδημαϊκής ταυτότητας (8)

Το νέο PIN θα πρέπει:

- Να έχει τουλάχιστον 4 χαρακτήρες
- Να είναι λιγότερο ή ίσο με 8 χαρακτήρες
- Να περιέχει μόνο αριθμητικούς χαρακτήρες

Βήμα 9ο :

Τέλος, εισάγουμε το νέο PIN (εις διπλούν) και επιλέγουμε «**Αλλαγή PIN Χρήστη**». Το PIN αλλάζει και η ακαδημαϊκή μας ταυτότητα είναι έτοιμη να χρησιμοποιηθεί.

3.4. ΔΙΑΔΙΚΑΣΙΑ ΕΚΔΟΣΗΣ ΨΗΦΙΑΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΤΥΠΟΥ CLASS A

Στην ενότητα αυτή θα παρουσιάσουμε την διαδικασία έκδοσης ψηφιακού πιστοποιητικού τύπου Α (**Class A)** στον φορέα του πρώην ΤΕΙ Στερεάς Ελλάδας, που αποτελεί την περίπτωση (case-study) εξετάζουμε εμείς στην παρούσα διπλωματική.

Πριν ξεκινήσει η διαδικασία, θα πρέπει να ικανοποιούνται οι παρακάτω προϋποθέσεις:

1. Να γίνει επιτόπια επίσκεψη του χρήστη στην αρχή καταχώρησης παρουσία του validator (συνήθως υπεύθυνος υπάλληλος Τμήματος Μηχανογράφησης) που έχει ορίσει ο Φορέας. Ο validator θα πρέπει να κάνει έλεγχο ταυτοπροσωπίας πριν εκδοθεί το πιστοποιητικό.

2. Ο χρήστης (διοικητικός υπάλληλος, καθηγητής, ειδικό τεχνικό προσωπικό) πρέπει να φέρει μαζί του:

- έγγραφο ταυτοπροσωπίας (αστυνομική ταυτότητα ή δίπλωμα οδήγησης ή διαβατήριο)
- ταυτότητα ή διαβατήριο σε ηλεκτρονική μορφή εικόνας (.png .jpg .jpeg),όπου θα πρέπει στο ίδιο αρχείο να αποτυπώνονται και οι 2 όψεις της ταυτότητας ή του διαβατηρίου (μπρος-πίσω)
- συμβατή κρυπτογραφική συσκευή (στην περίπτωσή μας την Ακαδημαϊκή Ταυτότητα).

3. Ο υπολογιστής που θα γίνει η αίτηση/παραλαβή πιστοποιητικού πρέπει να έχει ήδη εγκατεστημένους τους drivers της κρυπτογραφικής συσκευής (token, academic id).

4. Ως φυλλομετρητής θα πρέπει να χρησιμοποιηθεί ο Microsoft Internet Explorer.

Βήμα 1ο:

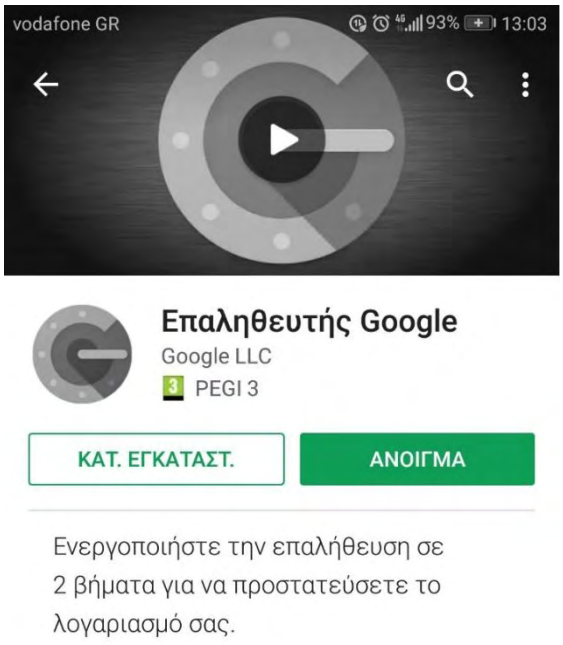
Έχοντας ικανοποιήσει όλα τα παραπάνω, εισέρχομαι στην ιστοσελίδα: **https://app.harica.gr/admin/login**

Από 24/10/2018 και σύμφωνα με τη νέα έκδοση των προδιαγραφών «Network Security Controls» (https://cabforum.org/wp-content/uploads/CABForum-Network-Security-Controls-1.2.pdf) που οφείλει να συμμορφώνεται η HARICA, οι validators των Φορέων θα πρέπει να κάνουν χρήση “Two-Factor Authentication (2FA)” (αυθεντικοποίηση δύο παραγόντων) όταν συνδέονται στο διαχειριστικό περιβάλλον για έγκριση/απόρριψη αιτημάτων πιστοποιητικών. Ουσιαστικά, με την ενεργοποίηση του 2FA, θα χρειάζεται κατά την είσοδο στη διαχειριστική σελίδα πέρα από το username / password να εισάγουμε και έναν κωδικό μιας χρήσης (One-Time Password – OTP) για μεγαλύτερη ασφάλεια.

Η διαδικασία ενεργοποίησης 2FA είναι απλή και χρειάζεται η εγκατάσταση ενός προγράμματος (Microsoft Authenticator, Google Authenticator ή άλλο) στο smartphone ή tablet που έχουμε. Η συγκεκριμένη λειτουργία ενεργοποιείται **την πρώτη φορά** που θα συνδεθούμε στο διαχειριστικό περιβάλλον του Φορέα μας.

Για να εγκαταστήσουμε το **"Google Authenticator" (Επαληθευτής Google)**, συνδεόμαστε από το κινητό στην εφαρμογή **"Google Play Store"(**Εφαρμογή λήψης Android εφαρμογών για κινητό**)** και κάνουμε αναζήτηση της εφαρμογής αυτής.

Εγκαθιστούμε την εφαρμογή **"Google Authenticator"** στην συσκευή μας και μόλις ολοκληρωθεί , επιλέγουμε άνοιγμα για να τρέξουμε την εφαρμογή:



Εικόνα 28: Επαληθευτής Google

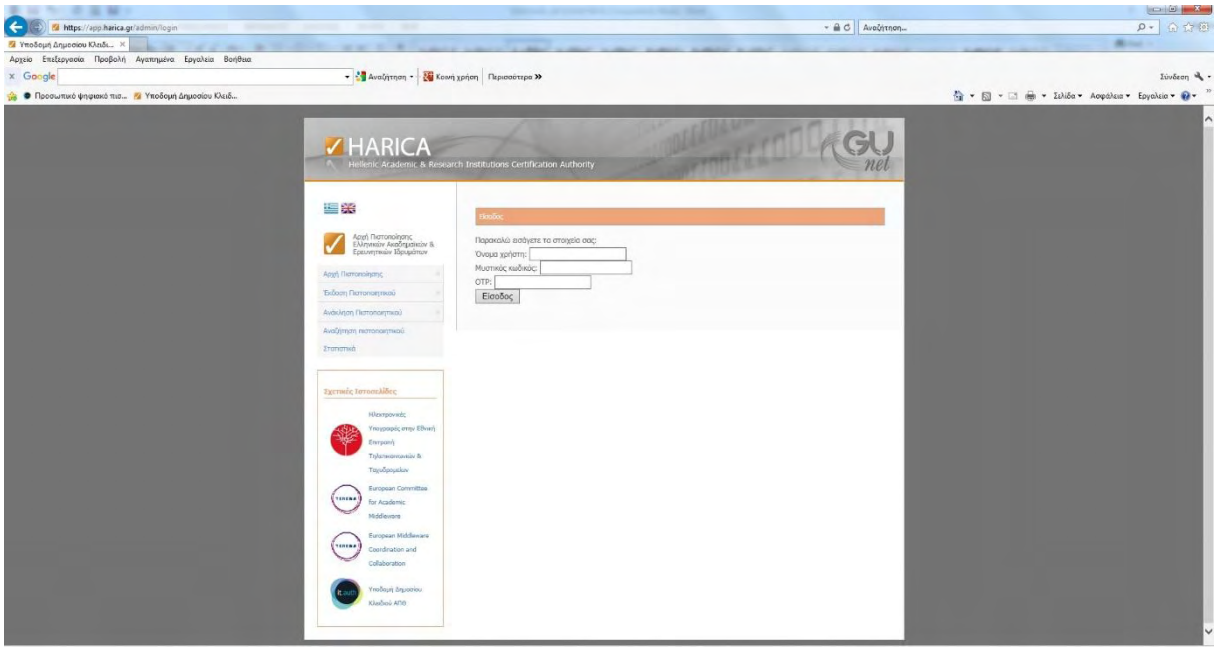
Συνδεόμαστε με τα στοιχεία μας του προσωπικού λογαριασμού μας στην Google και η εφαρμογή μας εγκαταστάθηκε:

Εικόνα 29: Επαληθευτής Google - Κωδικός HARICA

Σημείωση: Ο κωδικός αλλάζει κάθε λεπτό.

Βήμα 2ο:

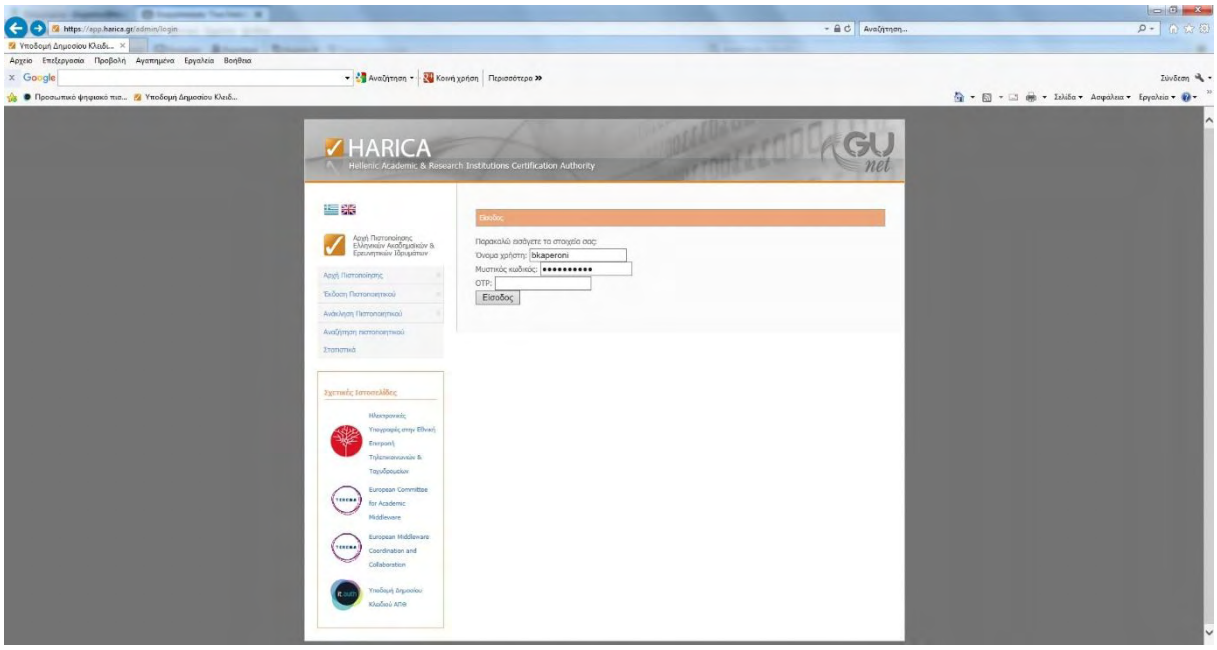
Έχοντας κάνει τα παραπάνω, μεταφερόμαστε ξανά στην αρχική οθόνη https://app.harica.gr/admin/login (Βλέπουμε ότι εμφανίζεται και το πεδίο OTP)



Εικόνα 30: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (1)

Βήμα 3ο:

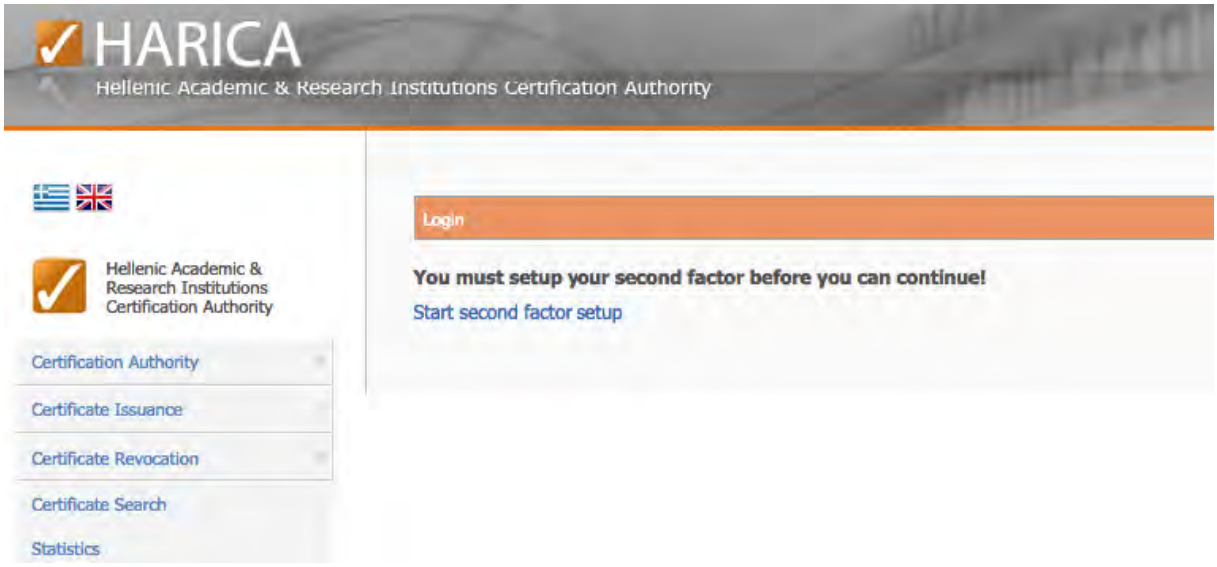
Δίνουμε το username / password, αφήνουμε το OTP κενό και επιλέγουμε Enter.



Εικόνα 31: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (2)

Βήμα 4ο:

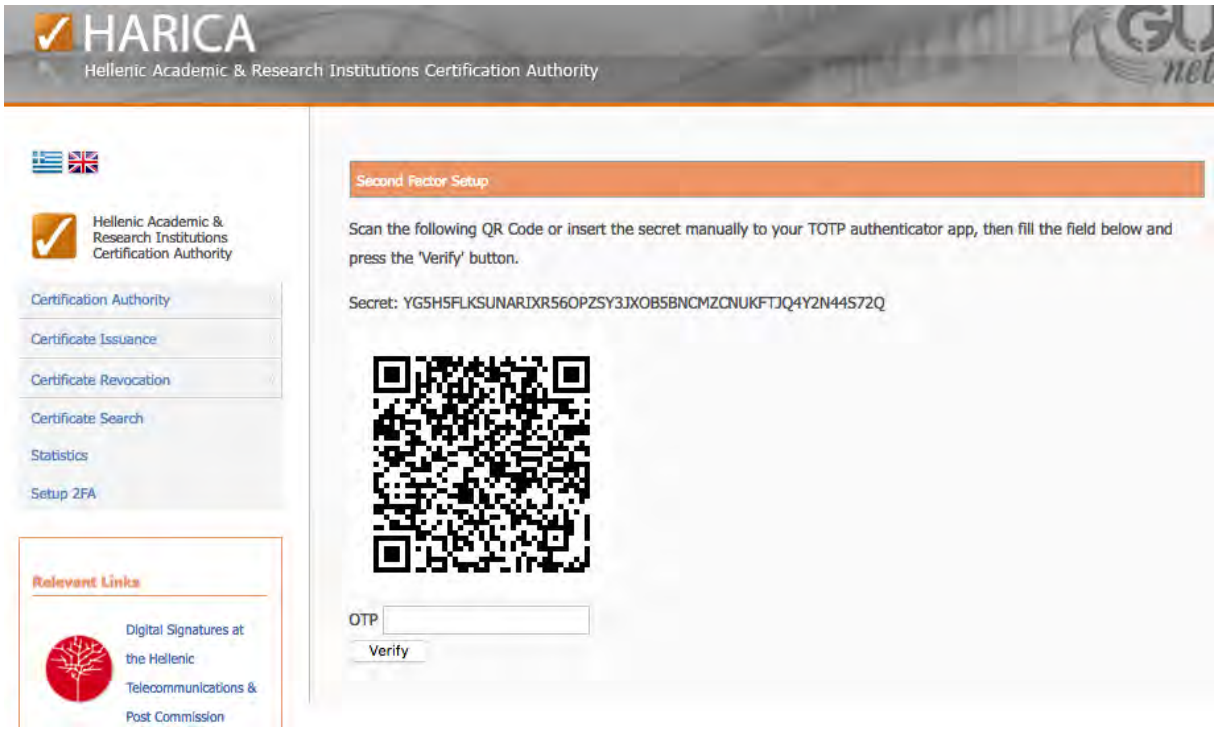
Στη συνέχεια μας βγάζει το παρακάτω μήνυμα και επιλέγουμε «**Start second factor setup**».



Εικόνα 32: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (3)

Βήμα 5ο:

Στη συνέχεια εμφανίζεται η παρακάτω σελίδα:

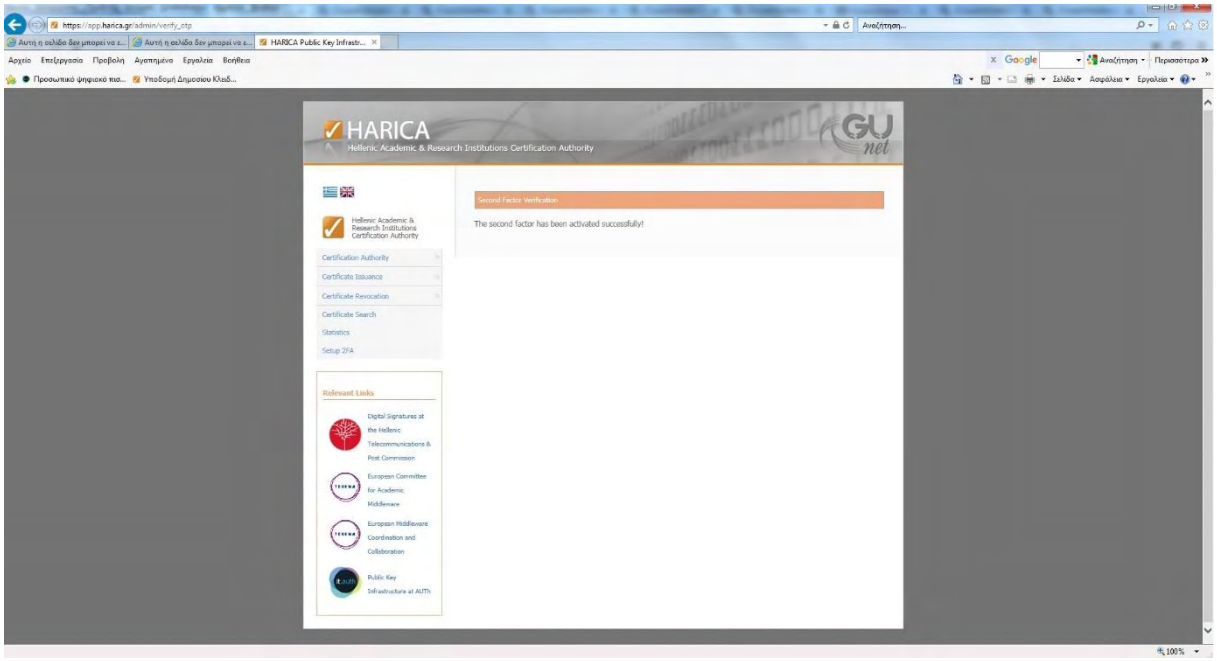


Εικόνα 33: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (4)

Βήμα 6ο:

Ανοίγουμε το πρόγραμμα που έχουμε κατεβάσει στη συσκευή μας και επιλέγουμε να προσθέσουμε ένα νέο λογαριασμό. Έχουμε τη δυνατότητα να εισάγουμε τον κωδικό Secret χειροκίνητα ή αυτόματα, σαρώνοντας το QR Code με την κάμερα της συσκευής μας.

Ο λογαριασμός έχει δημιουργηθεί με το όνομα HARICA και βλέπουμε τον κωδικό επαλήθευσης στη συσκευή μας. Συμπληρώνουμε το πεδίο OTP και επιλέγουμε Verify.

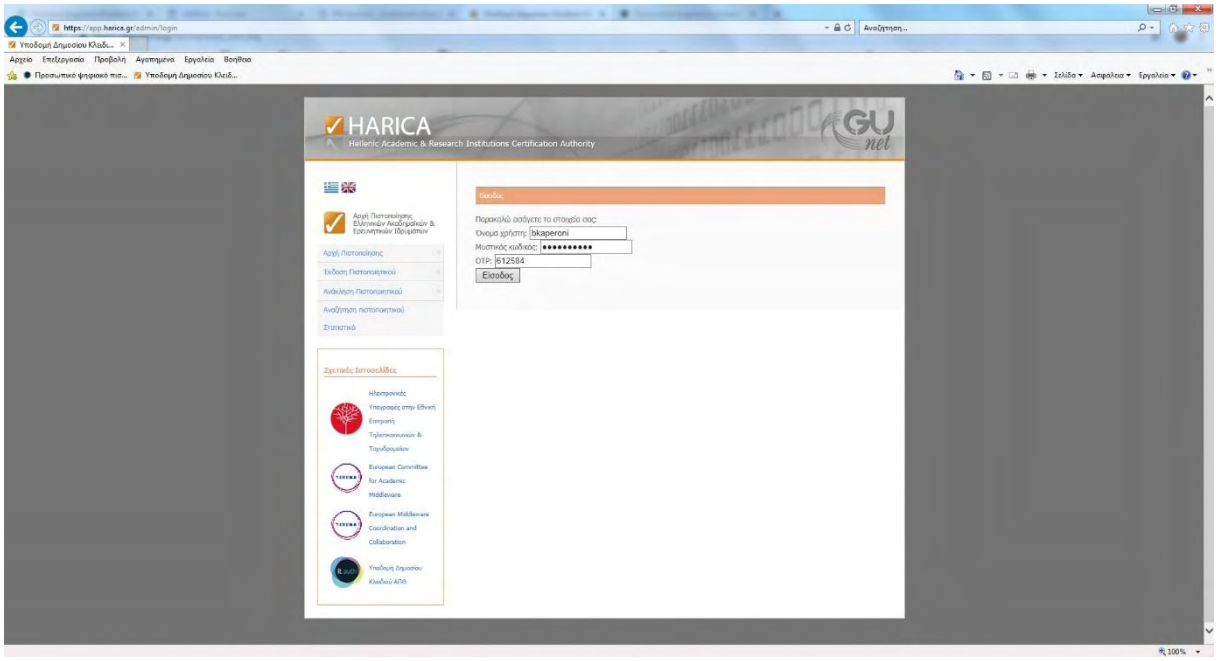


Εικόνα 34: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (5)

Η ρύθμιση έχει πραγματοποιηθεί και πλέον θα πρέπει να χρησιμοποιούμε τον κωδικό επαλήθευσης από την εφαρμογή.

Βήμα 7ο:

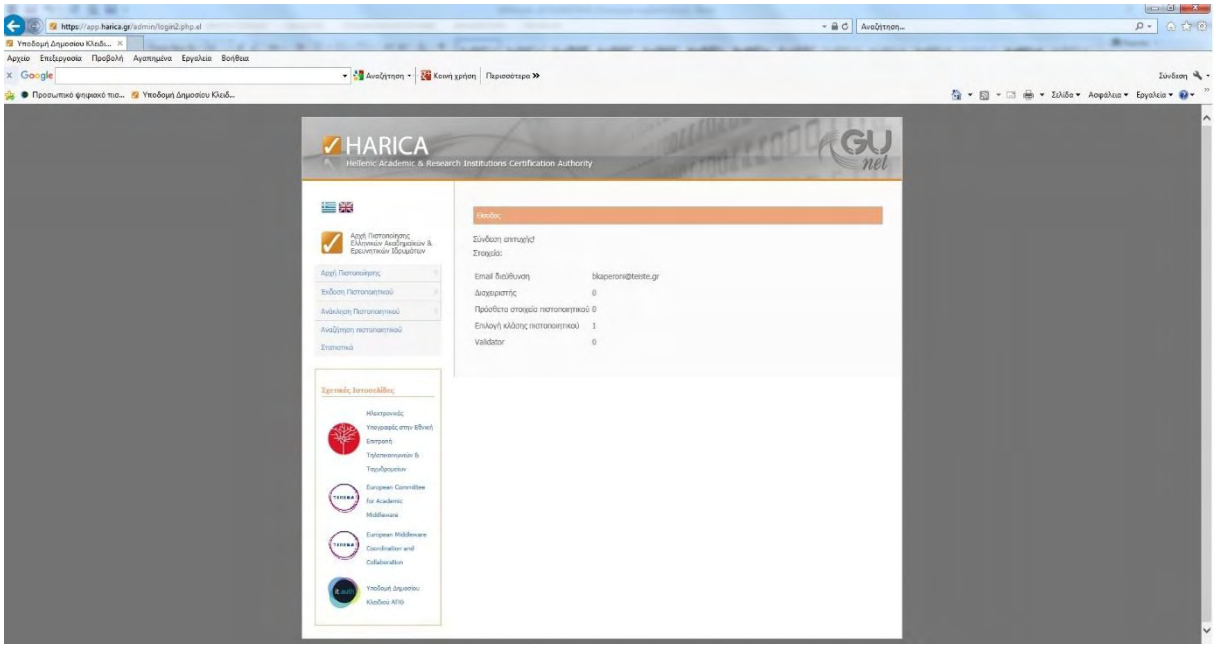
Εισάγω το όνομα χρήστη, τον μυστικό κωδικό μου και το OTP και επιλέγω Είσοδο:



Εικόνα 35: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (6)

Βήμα 8ο:

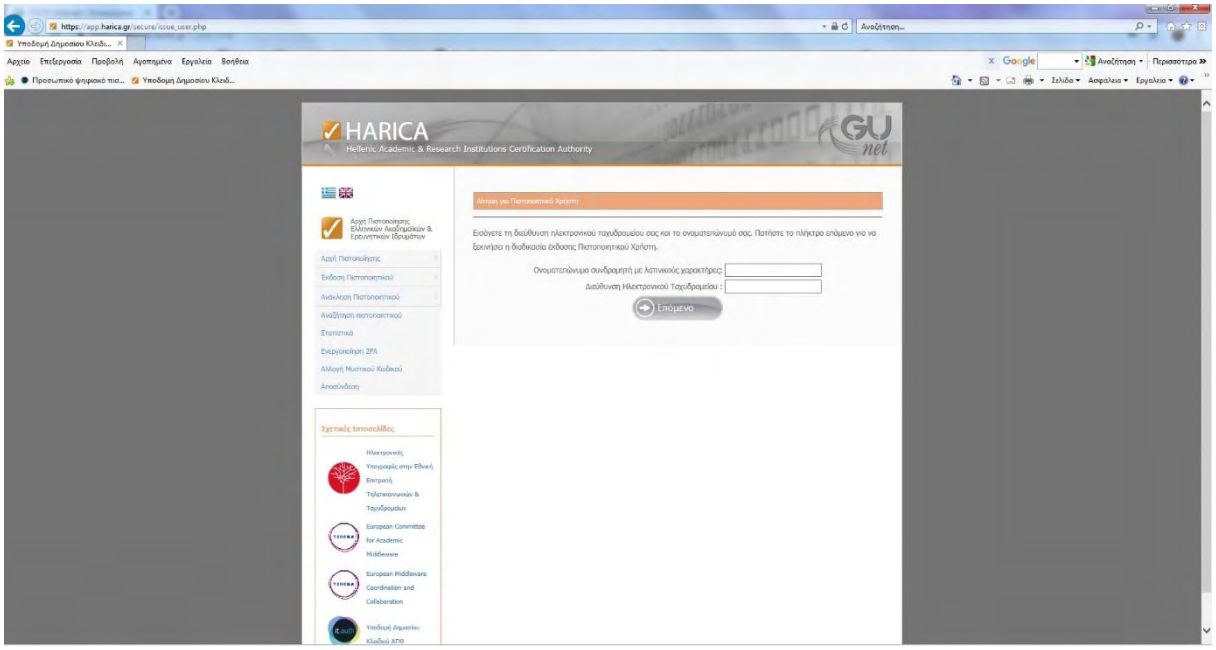
Εάν έχουμε εισάγει όλα τα στοιχεία σωστά, εμφανίζεται το μήνυμα «Σύνδεση επιτυχής!» και η παρακάτω σελίδα:



Εικόνα 36: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (7)

Βήμα 9ο:

Επιλέγω από το μενού Έκδοση Πιστοποιητικού -> Χρήστη:

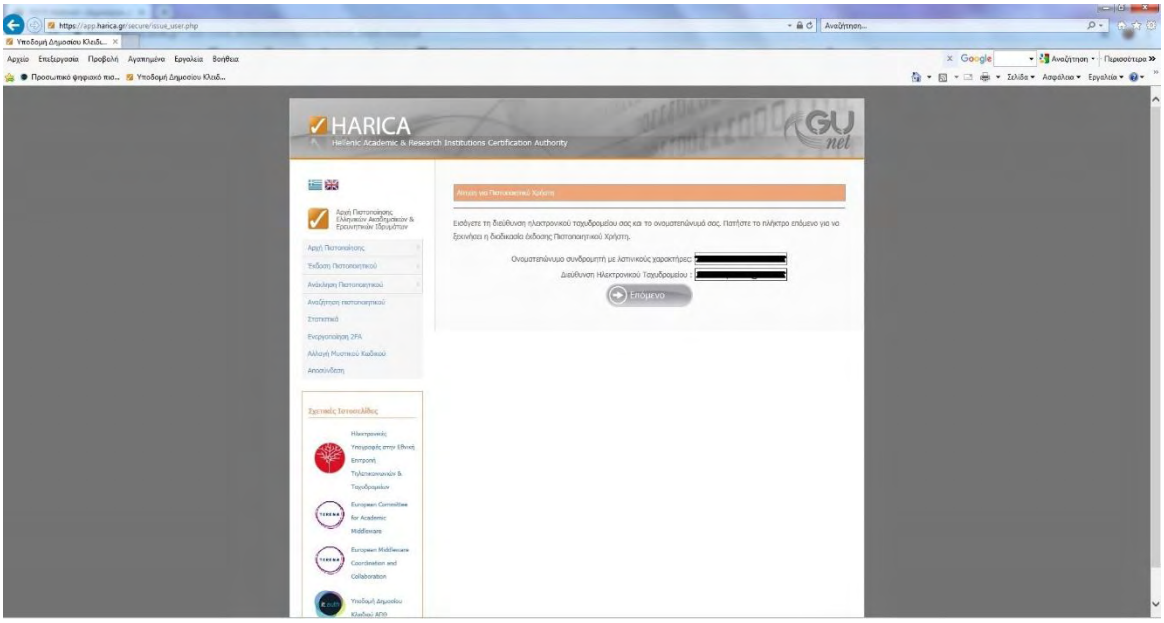


Εικόνα 37: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (8)

Βήμα 10ο:

Εισάγω: i) το ονοματεπώνυμο του χρήστη με λατινικούς χαρακτήρες και ii) την διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη (e-mail) για την οποία θα εκδοθεί το πιστοποιητικό (domain Φορέα - teiste) και επιλέγω Επόμενο.

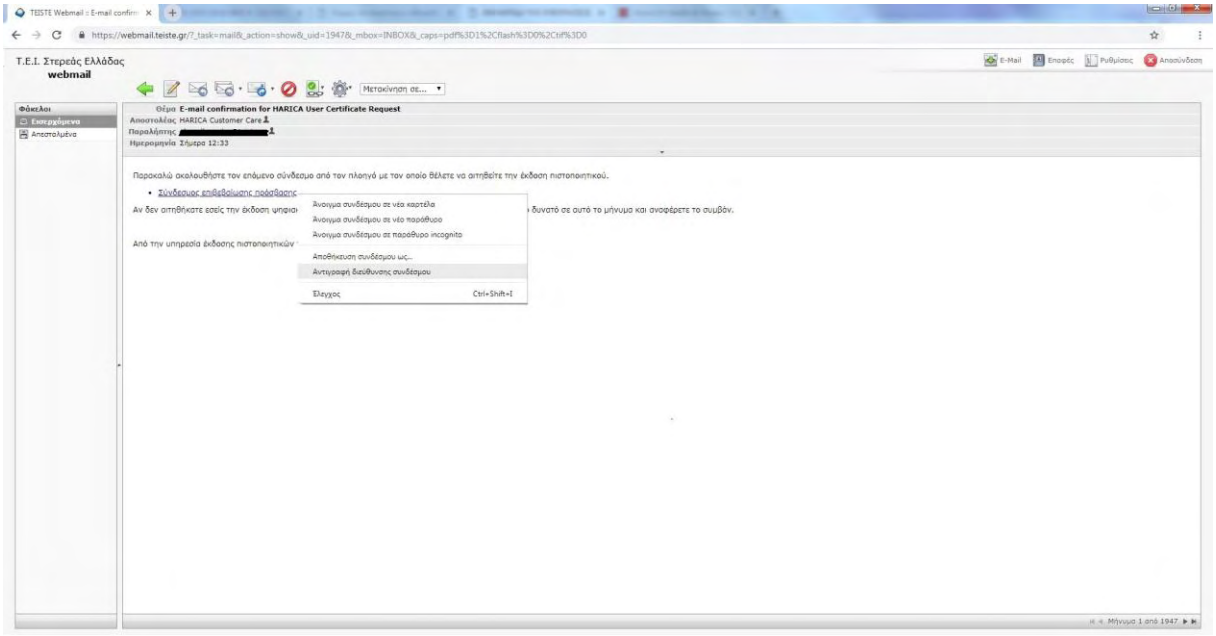
Σημείωση: Στην περίπτωσή μας έχει γίνει απόκρυψη των στοιχείων του χρήστη μας για προστασία των προσωπικών του δεδομένων.



Εικόνα 38: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (9)

Βήμα 11ο:

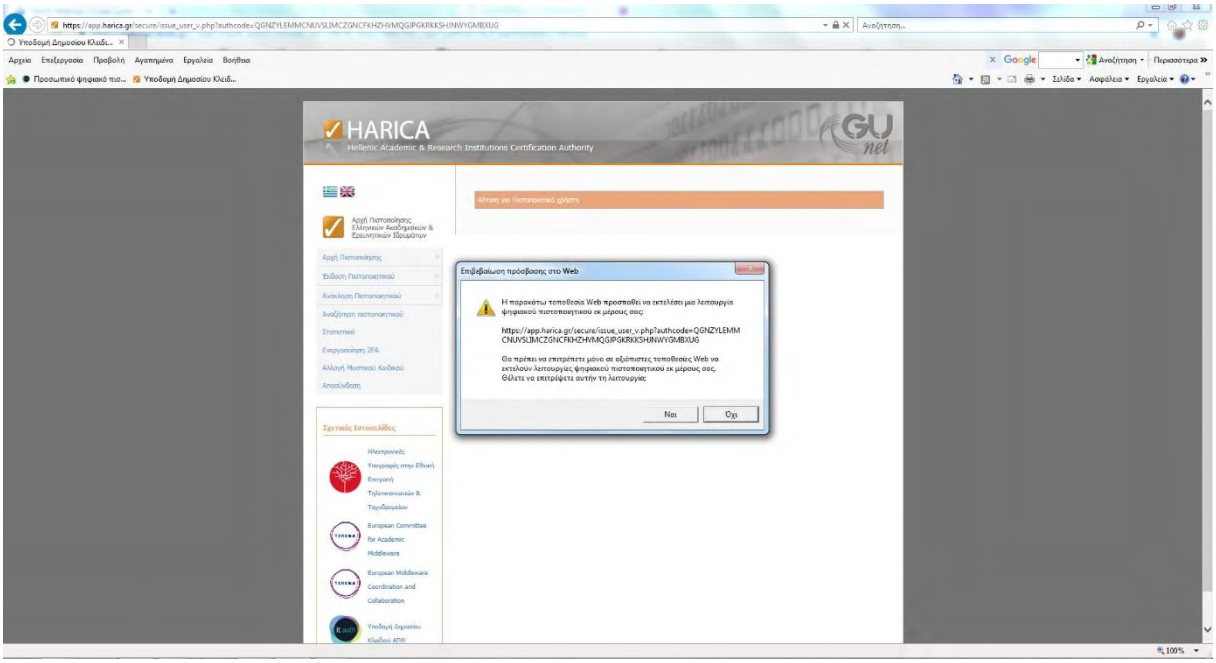
Ο χρήστης παραλαμβάνει e-mail στην διεύθυνση ηλεκτρονικού ταχυδρομείου του και επιλέγει κάνοντας «**Αντιγραφή τοποθεσίας συνδέσμου**» το «**Σύνδεσμος επιβεβαίωσης πρόσβασης».**



Εικόνα 39: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (10)

Βήμα 12ο:

Στην ιστοσελίδα του HARICA, κάνοντας «**Επικόλληση**» (**Σύνδεσμος επιβεβαίωσης πρόσβασης)** εμφανίζεται το προειδοποιητικό μήνυμα «**Επιβεβαίωση Πρόσβασης στο Web**» στο οποίο και επιλέγω **Ναι**.

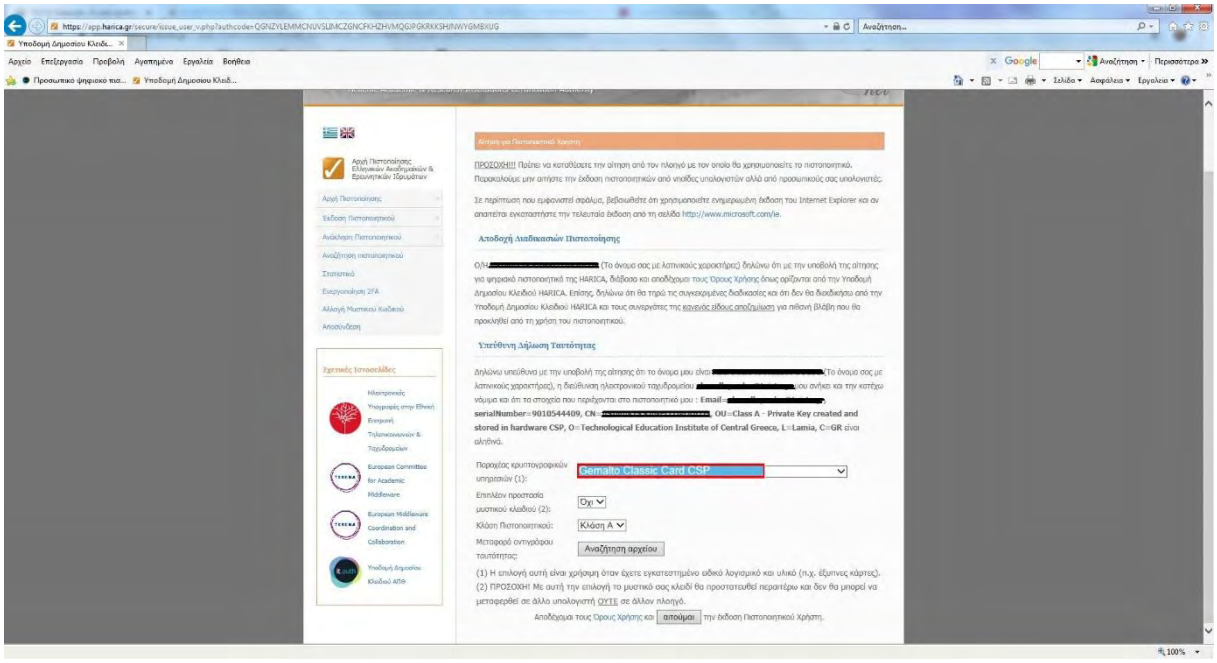


Εικόνα 40: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (11)

Βήμα 13ο:

Στη συνέχεια, ανοίγει η σελίδα αίτησης πιστοποιητικού, όπου ακολουθώ τα βήματα:

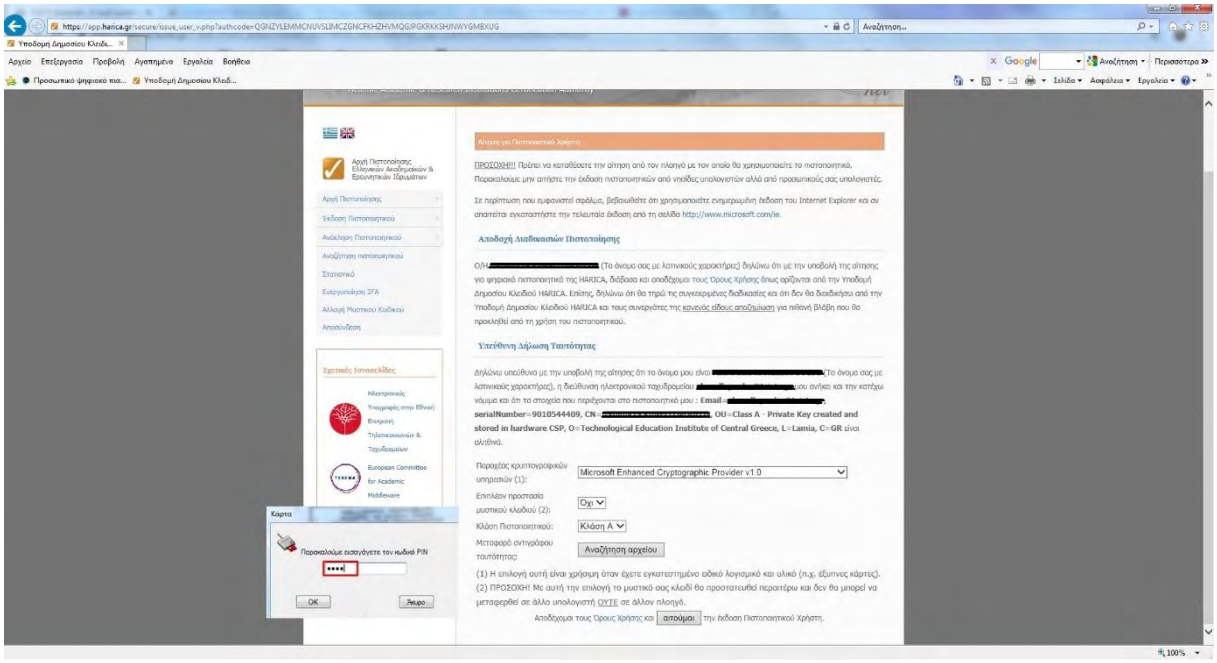
- Στον Παροχέα κρυπτογραφικών υπηρεσιών επιλέγω τον αντίστοιχο της Ακαδημαϊκής κάρτας (Gemalto Classic Card CSP) και
- Στην μεταφορά αντίγραφου ταυτότητας, κάνουμε μεταφόρτωση (upload) το ηλεκτρονικό αρχείο ταυτότητας σε μορφή εικόνας (.png .jpg .jpeg)
- Επιλέγω «αιτούμαι»



Εικόνα 41: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (12)

Βήμα 14ο:

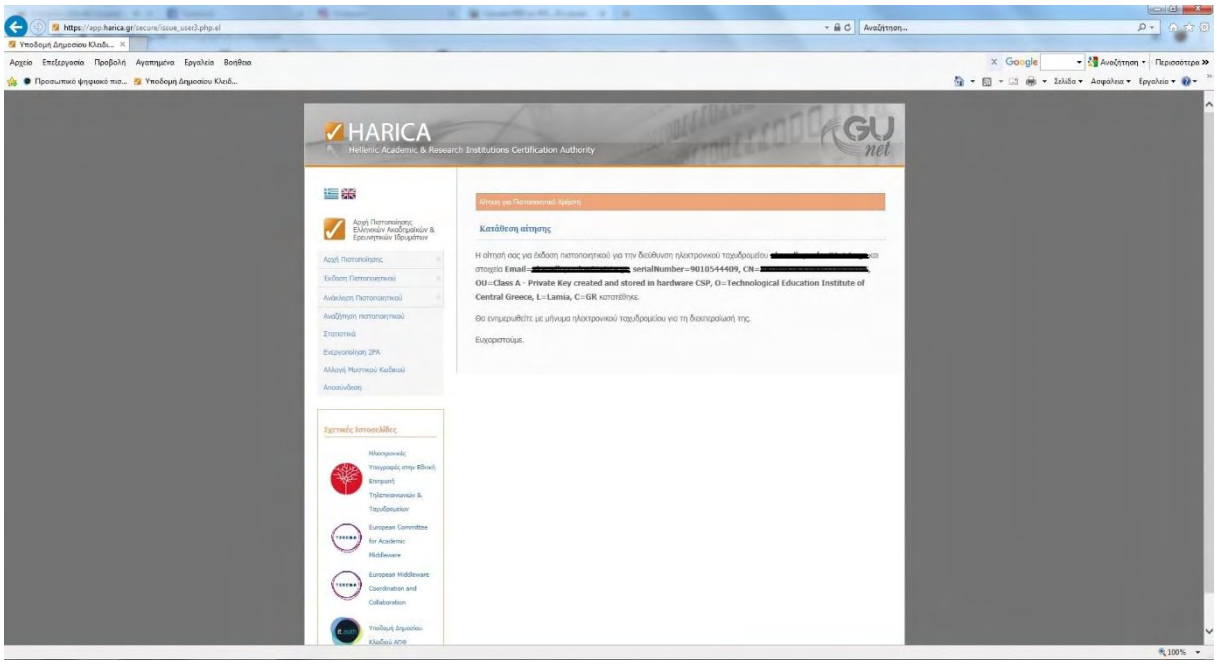
Ο χρήστης εισάγει τον κωδικό PIN της κάρτας του:



Εικόνα 42: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (13)

Βήμα 15ο:

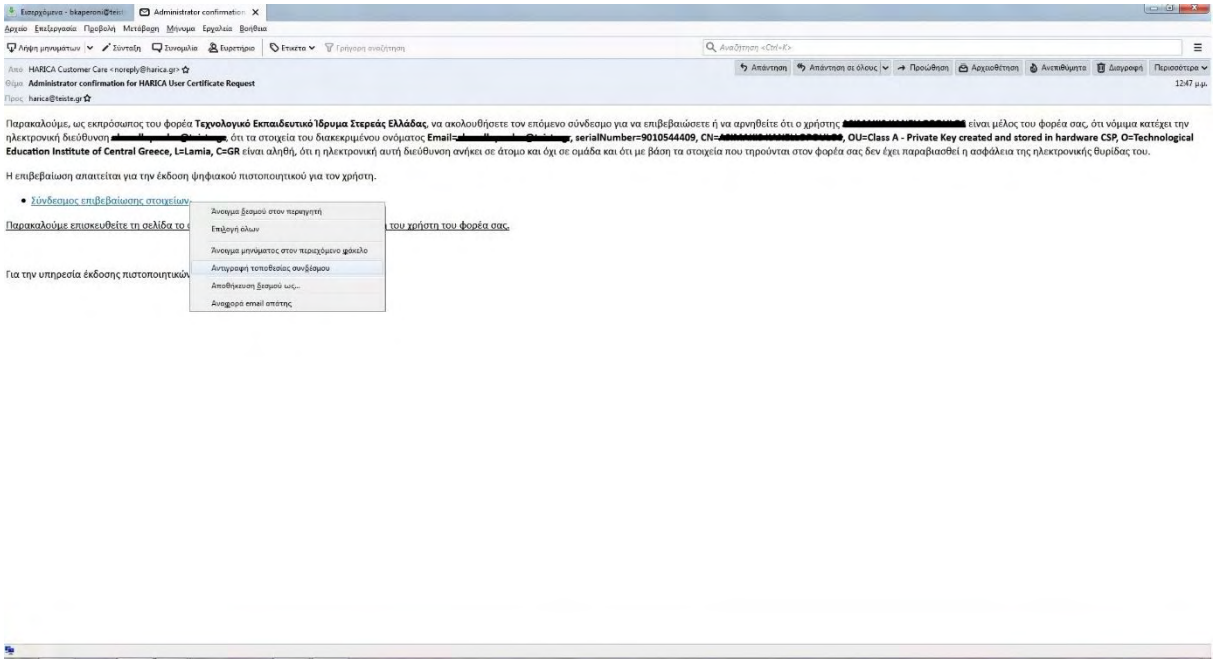
Εμφανίζεται η παρακάτω σελίδα «**Κατάθεσης αίτησης**» του χρήστη:



Εικόνα 43: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (14)

Βήμα 16ο:

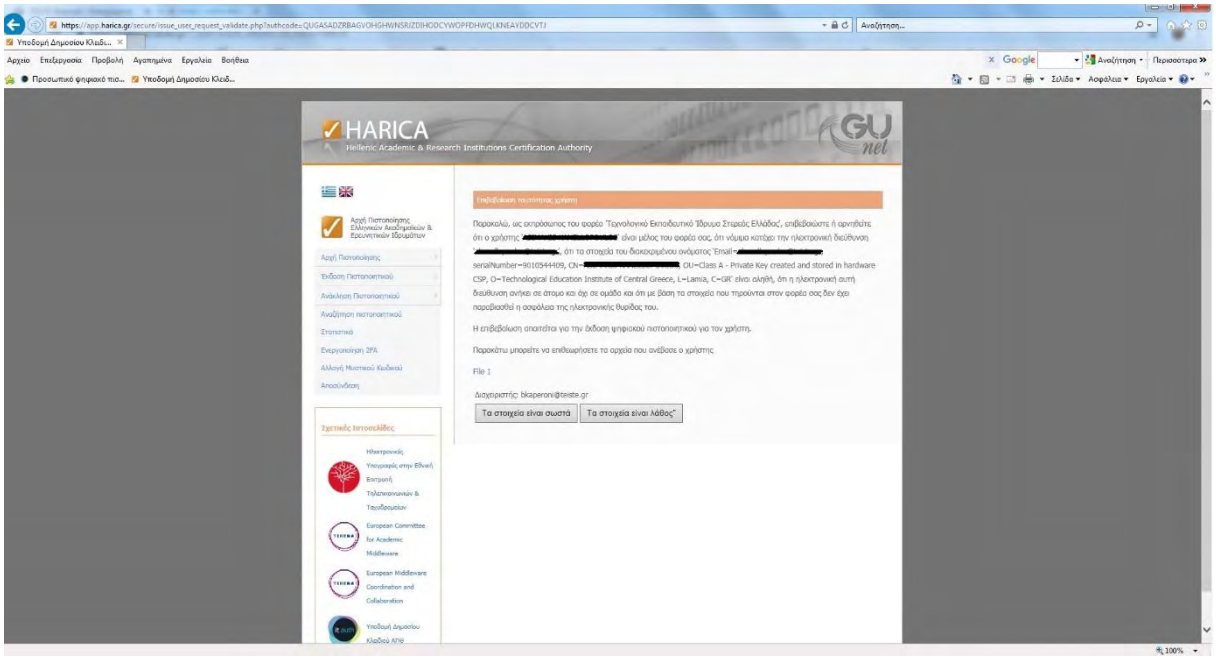
Ο validator παραλαμβάνει email και πατάει στο **«Σύνδεσμος επιβεβαίωσης στοιχείων»,** κάνοντας «**Αντιγραφή τοποθεσίας συνδέσμου**»**.**



Εικόνα 44: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (15)

Βήμα 17ο:

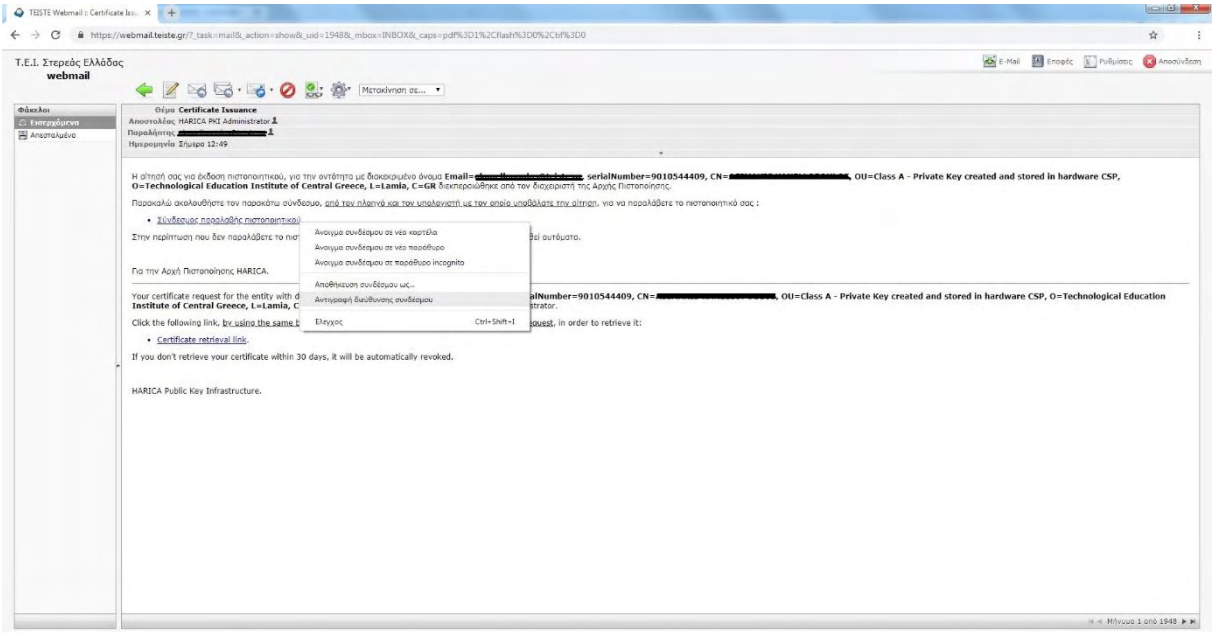
Ο validator, κάνοντας **«Επικόλληση»**, επιβεβαιώνει την ορθότητα των στοιχείων του χρήστη και εγκρίνει την έκδοση του πιστοποιητικού επιλέγοντας «**Τα στοιχεία είναι σωστά**».



Εικόνα 45: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (16)

Βήμα 18ο:

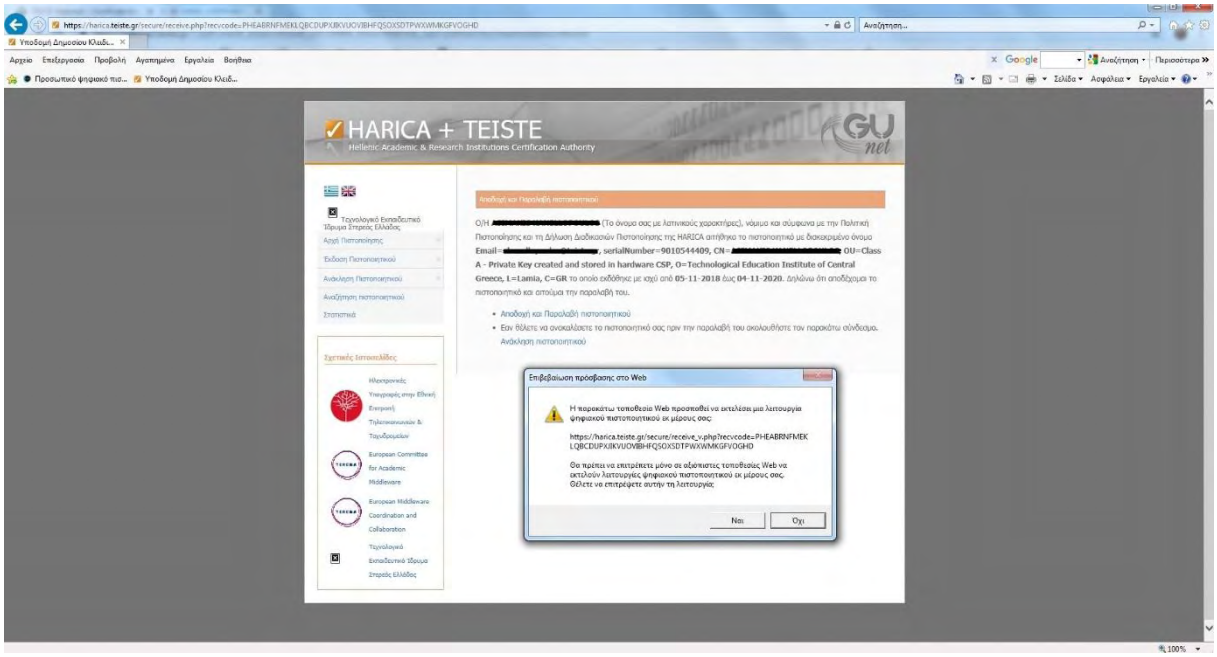
Ο χρήστης παραλαμβάνει e-mail στην διεύθυνση ηλεκτρονικού ταχυδρομείου του και επιλέγει, κάνοντας «**Αντιγραφή τοποθεσίας συνδέσμου**» στο **«Σύνδεσμος παραλαβής πιστοποιητικού»**.



Εικόνα 46: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (17)

Βήμα 19ο:

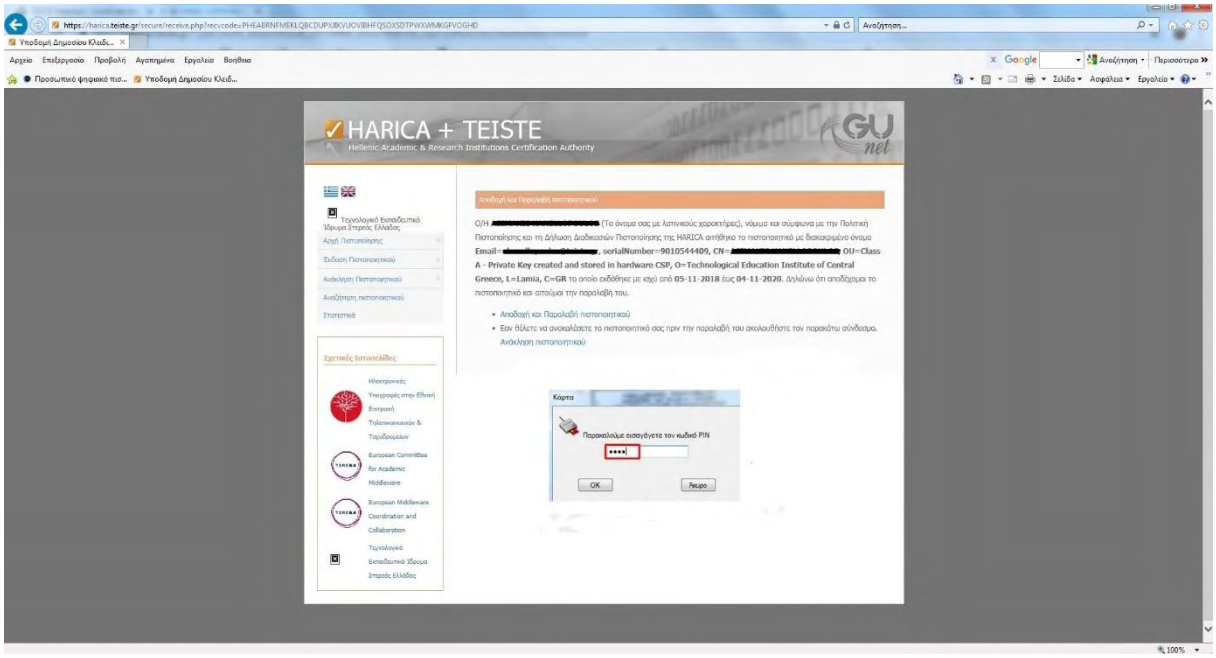
Στην ιστοσελίδα του HARICA, κάνοντας **«Επικόλληση»**, εμφανίζεται η σελίδα **«Αποδοχή και Παραλαβή πιστοποιητικού»** όπου ως validator επιβεβαιώνω την ορθότητα των στοιχείων του χρήστη και επιλέγω «**Αποδοχή και Παραλαβή πιστοποιητικού**». Στο προειδοποιητικό μήνυμα **«Επιβεβαίωση Πρόσβασης στο Web»** επιλέγω **Ναι**.



Εικόνα 47: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (18)

Βήμα 20ο:

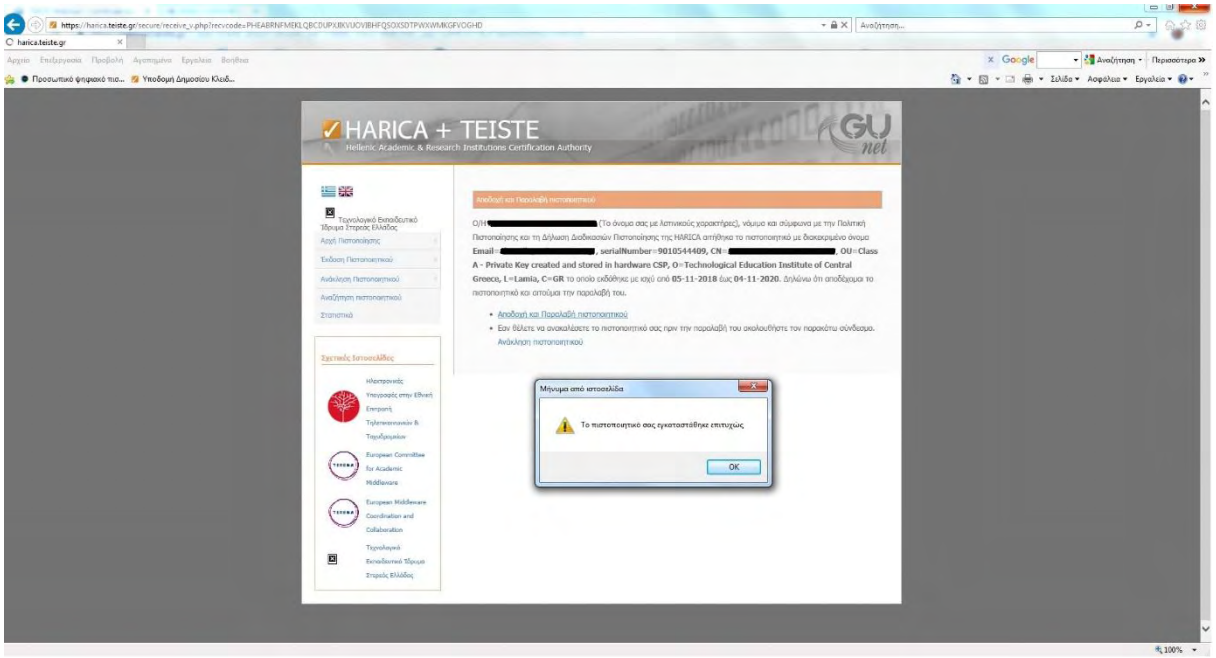
Ο χρήστης εισάγει τον κωδικό PIN της κάρτας του:



Εικόνα 48: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (19)

Βήμα 21ο:

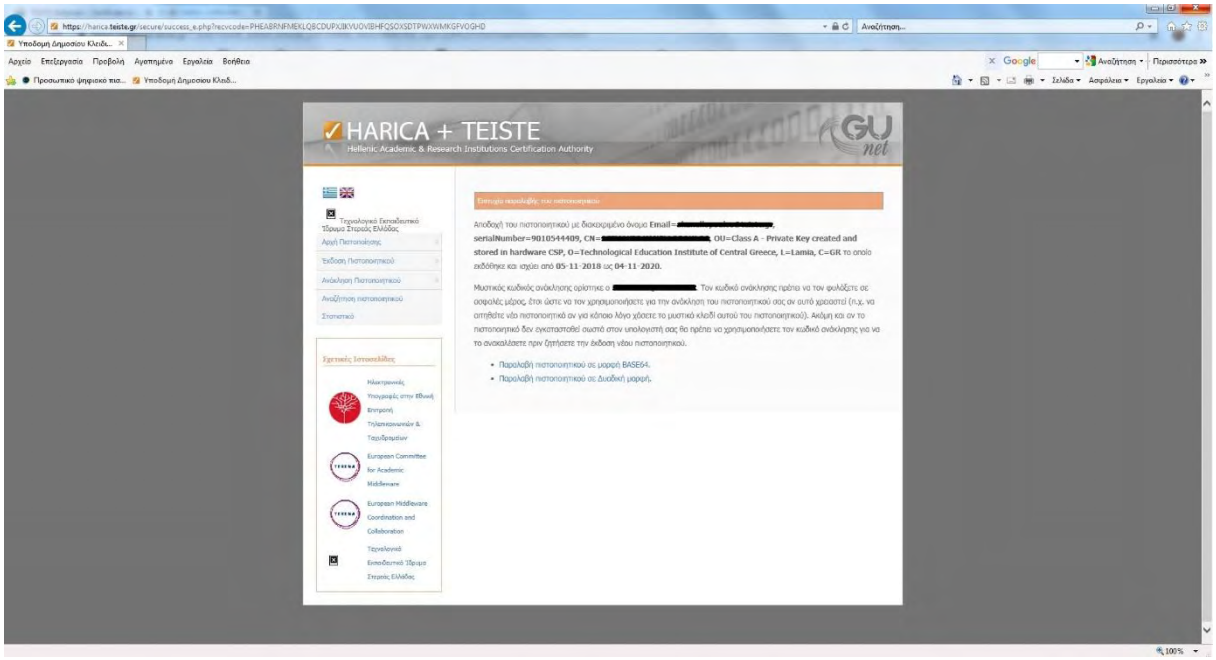
Το πιστοποιητικό του χρήστη έχει εγκατασταθεί επιτυχώς.



Εικόνα 49: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (20)

Βήμα 22ο:

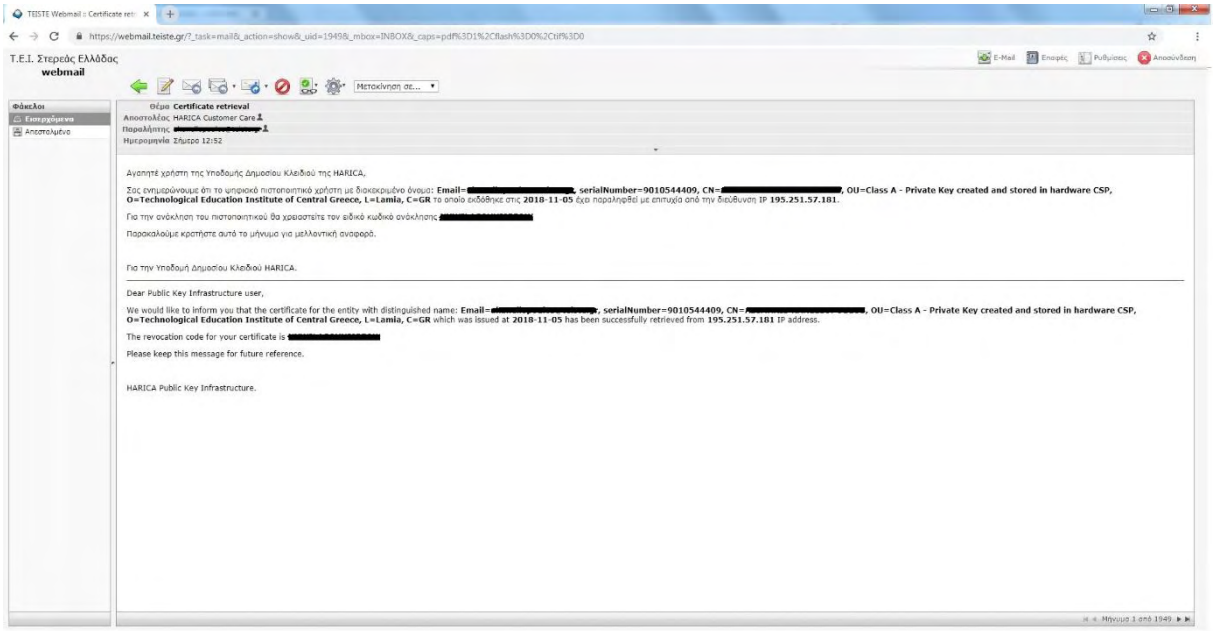
Στη σελίδα που εμφανίζεται υπάρχει και ο μυστικός κωδικός ανάκλησης, τον οποίο αποθηκεύει ο χρήστης για μελλοντική χρήση.



Εικόνα 50: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (21)

Βήμα 23ο:

Ο χρήστης παραλαμβάνει e-mail στην διεύθυνση ηλεκτρονικού ταχυδρομείου του για την επιτυχή έκδοση του πιστοποιητικού του και του ειδικού (μυστικού) κωδικού ανάκλησής του, το οποίο και αποθηκεύει κάπου σε περίπτωση μελλοντικής χρήσης.



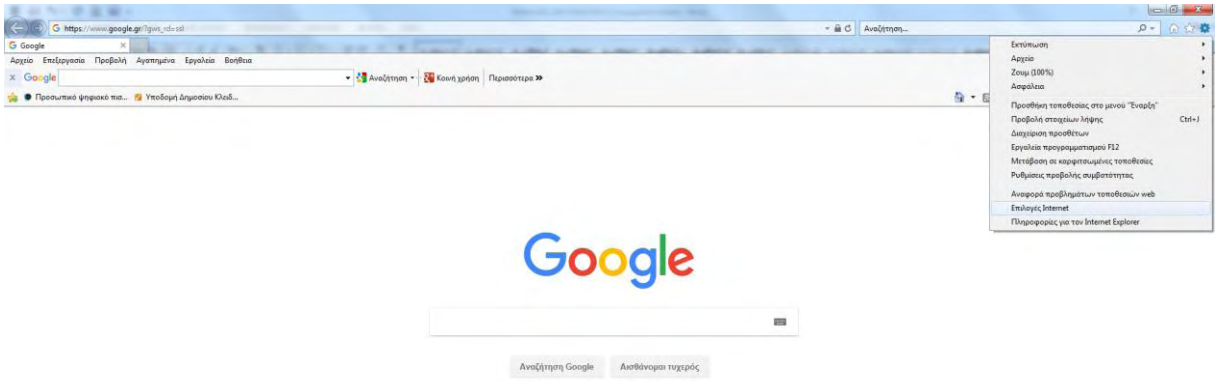
Εικόνα 51: Στιγμιότυπο οθόνης έκδοσης ηλεκτρονικής υπογραφής μέσω HARICA (22)

3.5. ΈΛΕΓΧΟΣ ΑΠΟΘΗΚΕΥΣΗΣ ΠΡΟΣΩΠΙΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΕ ΛΟΓΙΣΜΙΚΟ WINDOWS

Στην ενότητα αυτή, θα περιγράψουμε πως ελέγχουμε αν στο χώρο αποθήκευσης πιστοποιητικών των Windows, υπάρχει αποθηκευμένο το προσωπικό πιστοποιητικό μας (τύπου class B).

Βήμα 1ο:

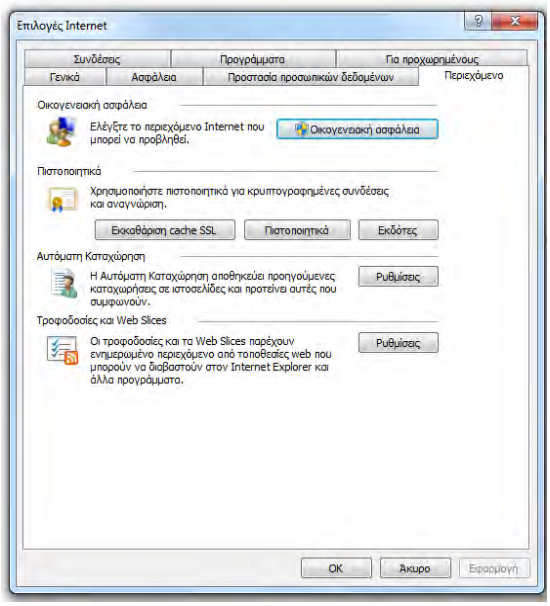
Αρχικά, ανοίγουμε τον φυλλομετρητή (browser) του Internet Explorer και επιλέγουμε το γρανάζι δεξιά του παραθύρου. Στη συνέχεια, κάνουμε κλικ στις Επιλογές Internet / Internet Options.



Εικόνα 52: Έλεγχος Αποθήκευσης Προσωπικού Πιστοποιητικού - Επιλογές Internet

Βήμα 2ο:

Στην συνέχεια, επιλέγουμε την καρτέλα Περιεχόμενο / Content κι από εκεί επιλέγουμε Πιστοποιητικά / Certificates.

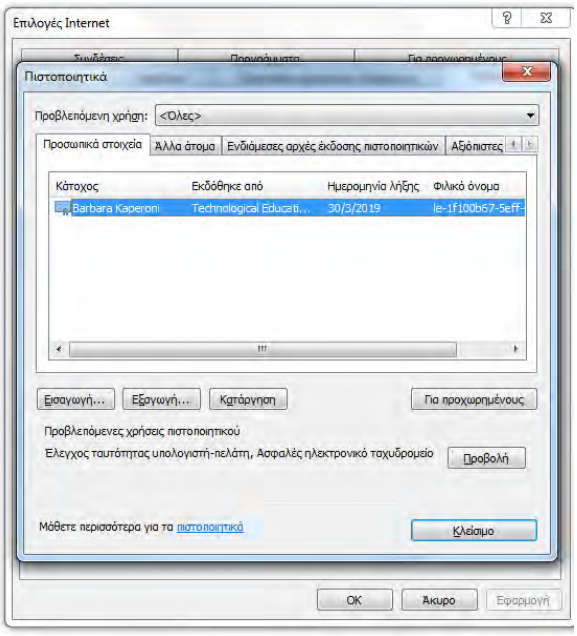


Εικόνα 53: Έλεγχος Αποθήκευσης Προσωπικού Πιστοποιητικού - Επιλογές Internet - Περιεχόμενο - Πιστοποιητικά

Βήμα 3ο:

Τέλος, επιλέγουμε την καρτέλα Προσωπικά / Personal όπου παρουσιάζονται όλα τα πιστοποιητικά που έχουν αποθηκευτεί, μαζί με κάποια στοιχεία που προσδιορίζουν κάθε

πιστοποιητικό όπως από ποιον εκδόθηκε και την ημερομηνία Λήξης/Expiration Date της ισχύος του.



Εικόνα 54: Έλεγχος Αποθήκευσης Προσωπικού Πιστοποιητικού - Επιλογές Internet - Προσωπικά στοιχεία

3.6. ΈΛΕΓΧΟΣ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΣΤΗΝ ΑΚΑΔΗΜΑΪΚΗ ΤΑΥΤΟΤΗΤΑ

Στην ενότητα αυτή, θα περιγράψουμε πως ελέγχουμε στην ακαδημαϊκή μας ταυτότητα, υπάρχει αποθηκευμένο το προσωπικό μας πιστοποιητικό (τύπου class A).

Βήμα 1ο:

Αρχικά, συνδέουμε τον αναγνώστη καρτών, έχοντας τοποθετήσει σε αυτόν την ακαδημαϊκή μας ταυτότητα.

Βήμα 2ο:

Το εικονίδιο που απεικονίζει τον καρταναγνώστη (card reader) θα αλλάξει μορφή, όπως φαίνεται και στο παρακάτω στιγμιότυπο, άρα θα μπορέσουμε να χρησιμοποιήσουμε την ακαδημαϊκή μας ταυτότητα.

Εικόνα 55: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (1)

Βήμα 3ο:

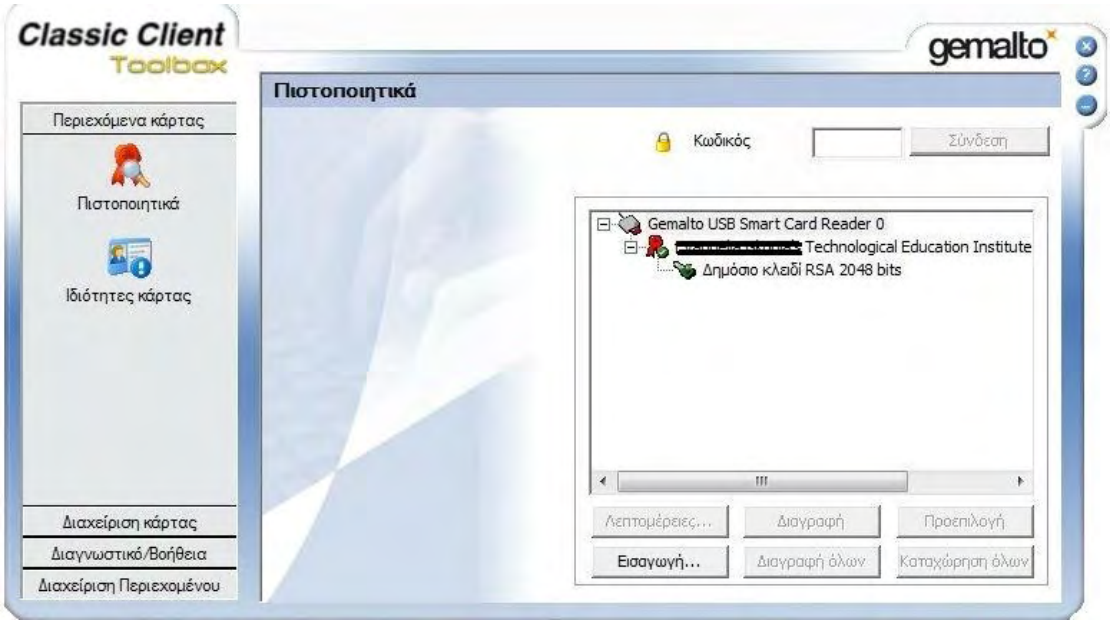
Κάνουμε διπλό κλικ στο εικονίδιο αυτό και ανοίγει το παρακάτω παράθυρο:

Εικόνα 56: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (2)

Βήμα 4ο:

Κάνουμε κλικ στο εικονίδιο «**Πιστοποιητικά**» όπου και βλέπουμε το Δημόσιο κλειδί του πιστοποιητικού μας:

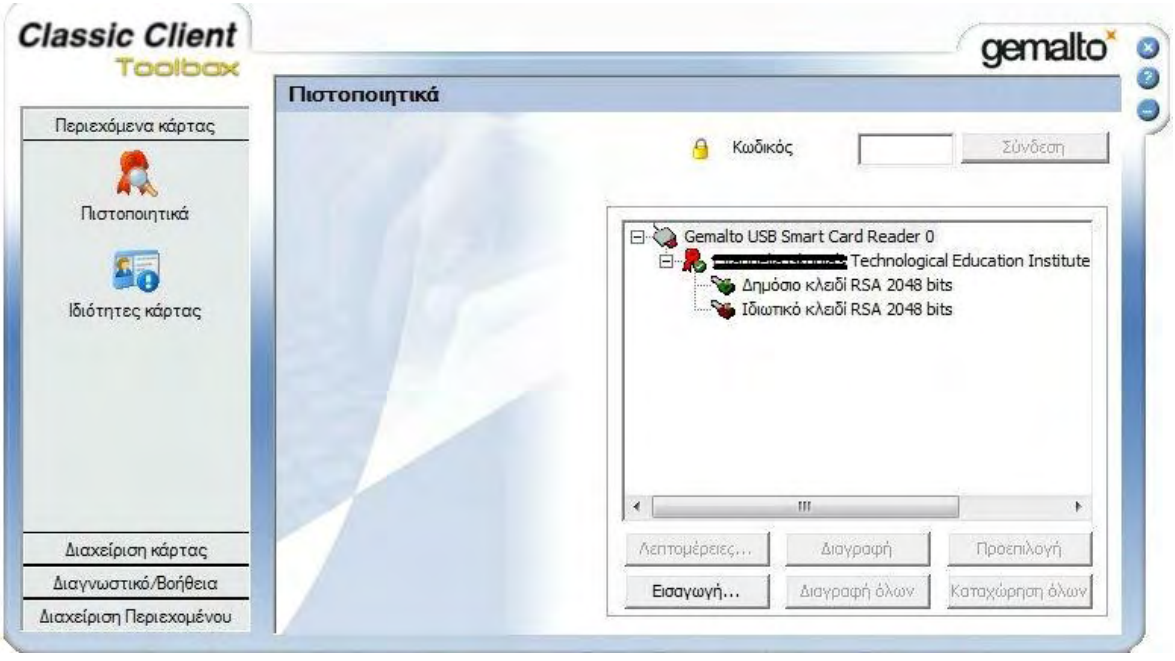
Σημείωση: Στην περίπτωσή μας δεν φαίνεται το ονοματεπώνυμο του χρήστη μας για προστασία των προσωπικών του δεδομένων.



Εικόνα 57: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (3)

Βήμα 5ο:

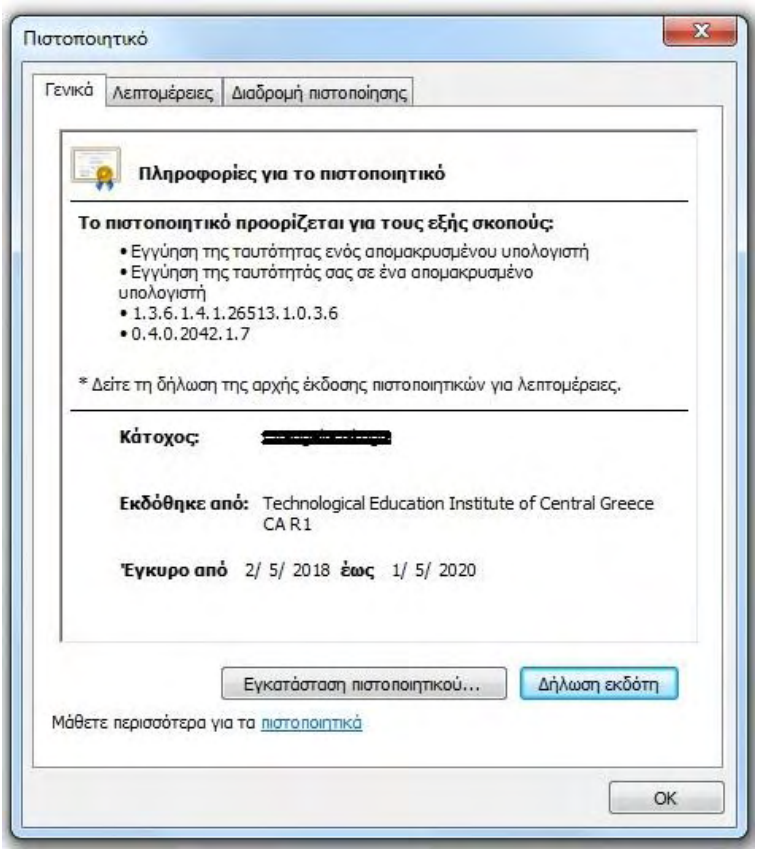
Εισάγουμε το PIN (κωδικό) της κάρτας και επιλέγουμε σύνδεση. Έτσι εμφανίζεται και το Ιδιωτικό κλειδί του πιστοποιητικού μας.



Εικόνα 58: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (4)

Βήμα 6ο:

Επιλέγουμε το πιστοποιητικό και στη συνέχεια, κάνουμε κλικ στο κουμπί **Λεπτομέρειες**, όπου εκεί παρέχονται κάποιες πληροφορίες αναφορικά με το πιστοποιητικό μας.



Εικόνα 59: Στιγμιότυπο οθόνης ελέγχου προσωπικού πιστοποιητικού στην ακαδημαϊκή ταυτότητα (5)

3.7. ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ PDF ΑΡΧΕΙΟΥ ΜΕ ΤΗ ΧΡΗΣΗ ΤΟΥ ADOBE READER

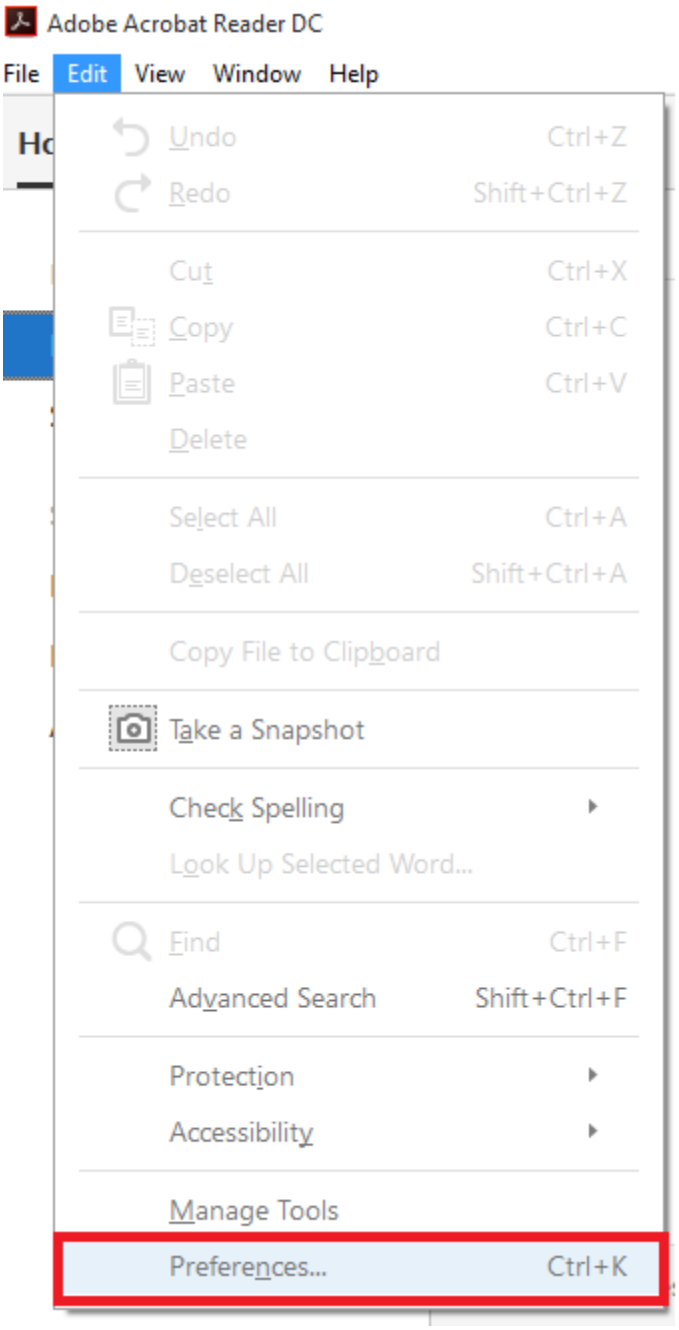
Στην ενότητα αυτή, περιγράφεται η διαδικασία που ακολουθείται ώστε να επιτευχθεί η προσθήκη εγκεκριμένης ψηφιακής υπογραφής σε έγγραφα pdf και σε περιβάλλον Windows, όπως ορίζεται από το ΠΔ 150/2001 και από τον Ευρωπαϊκό Κανονισμό 910/2014.

Για τον σκοπό αυτό, συνδέουμε την ακαδημαϊκή μας ταυτότητα στον υπολογιστή μας και χρησιμοποιούμε την έκδοση προγράμματος Adobe Reader DC.

Βήμα 1ο:

Αρχικά, θα πρέπει να ρυθμίσουμε τον Διακομιστή Χρονοσήμανσης[21].

Έτσι, ανοίγουμε το πρόγραμμα **Adobe Reader DC** κι επιλέγουμε **Edit -> Preferences.**

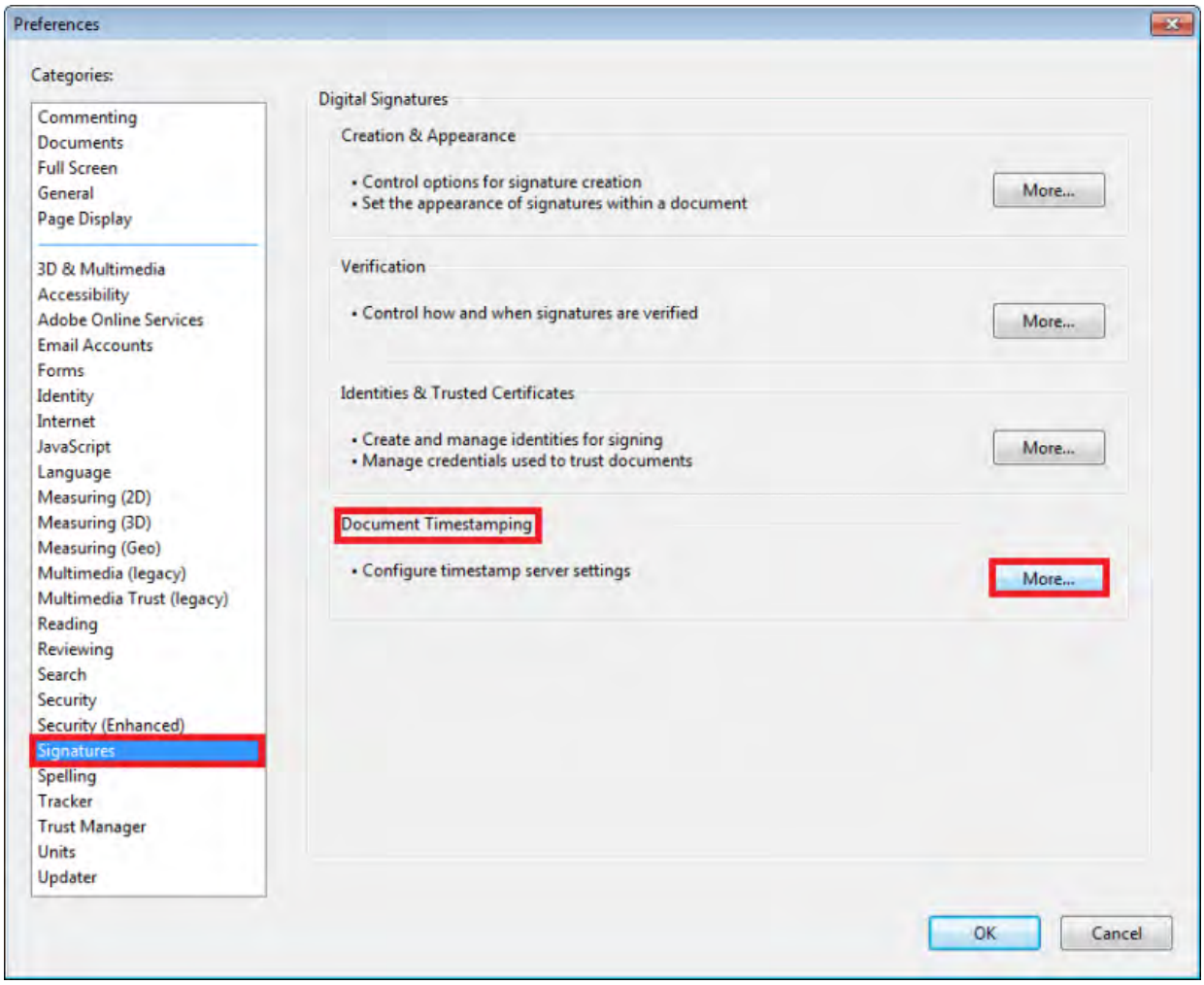


Εικόνα 60: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (1)

[21]Τεκμήριο απόδειξης ότι σε μία συγκεκριμένη χρονική στιγμή, υπήρχε ένα σύνολο ψηφιακών δεδομένων.

Βήμα 2ο:

Επιλέγουμε **Signatures->Document Timestamping**[22]**->More**.



Εικόνα 61: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (2)

Βήμα 3ο:

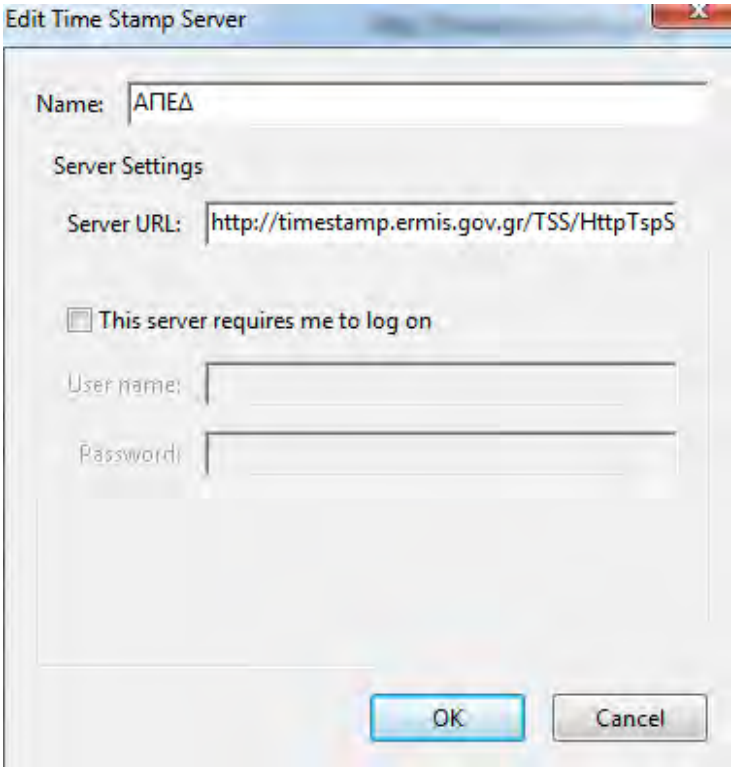
Στο παράθυρο που εμφανίζεται επιλέγουμε **New**.

Στην δικιά μας περίπτωση, θα χρησιμοποιηθεί ο διακομιστής χρονοσήμανσης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ):

[22]Η πληροφορία της διασύνδεσης ενός εγγράφου με την ακριβή ώρας δημιουργίας του παρέχεται από την ψηφιακή χρονοσφραγίδα (digital timestamp).

Name	ΑΠΕΔ
Server URL	http://timestamp.Ermis.gov.gr/TSS/HttpTspServer

Εικόνα 62: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (3)

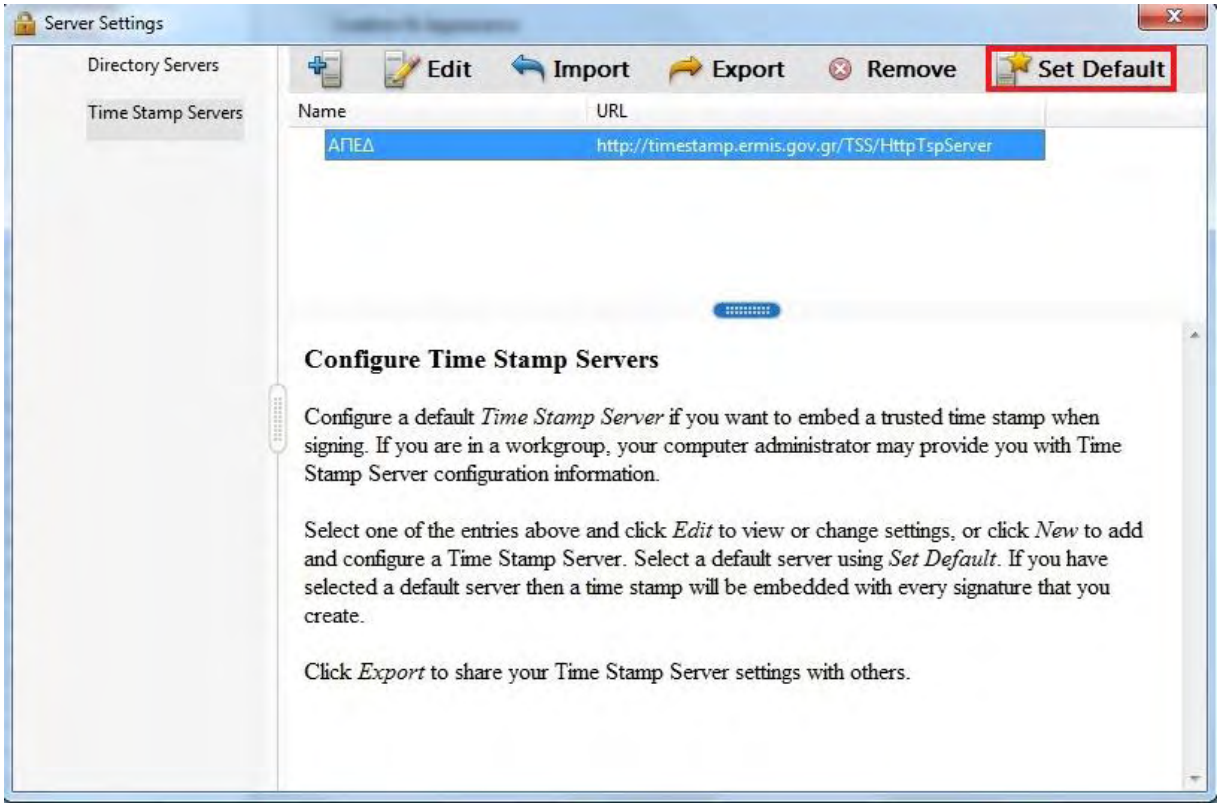


Εικόνα 63: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (4)

Στη συνέχεια, επιλέγουμε **OK**.

Βήμα 4ο:

Κάνοντας κλικ στον **Set Default**, ορίζουμε ως προεπιλογή στον διακομιστή χρονοσήμανσης που ρυθμίσαμε πριν (ΑΠΕΔ). Επιλέγουμε **OK** και κατόπιν κλείνουμε το παράθυρο.



Εικόνα 64: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (5)

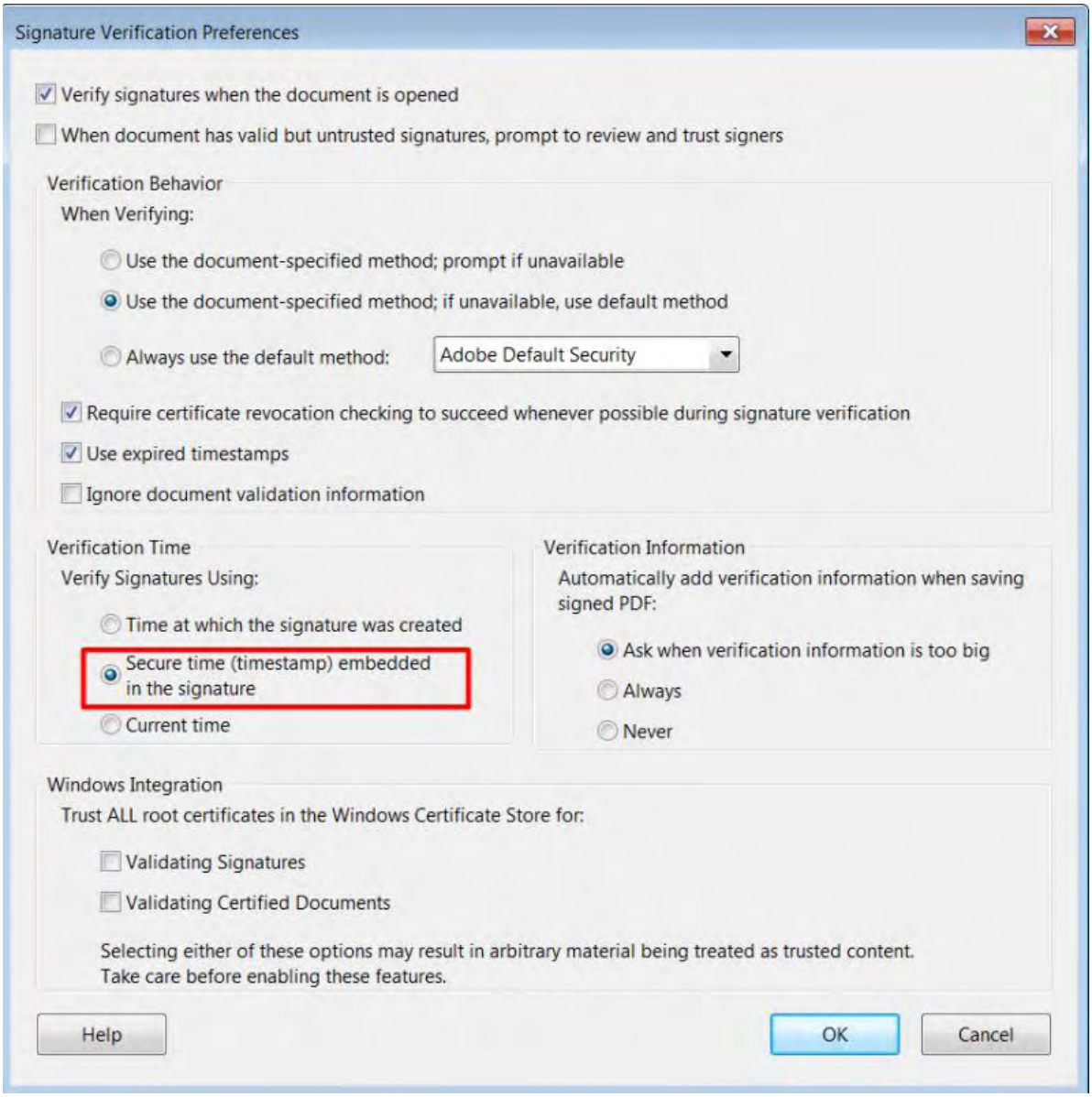
Βήμα 5ο:

Επιλέγουμε από την καρτέλα **Preferences->Signatures->Verification->More**.

Στην καρτέλα **Signature Verification Preferences** και στο πεδίο**Verification Time** επιλέγουμε το **Secure time (timestamp) embedded in the signature**.

Αυτό γίνεται γιατί θα πρέπει η ημερομηνία της ψηφιακής μας υπογραφής να προκύπτει από τον διακομιστή χρονοσήμανσης, όπως έχει οριστεί σε παραπάνω βήμα.

Πατάμε **OK**.

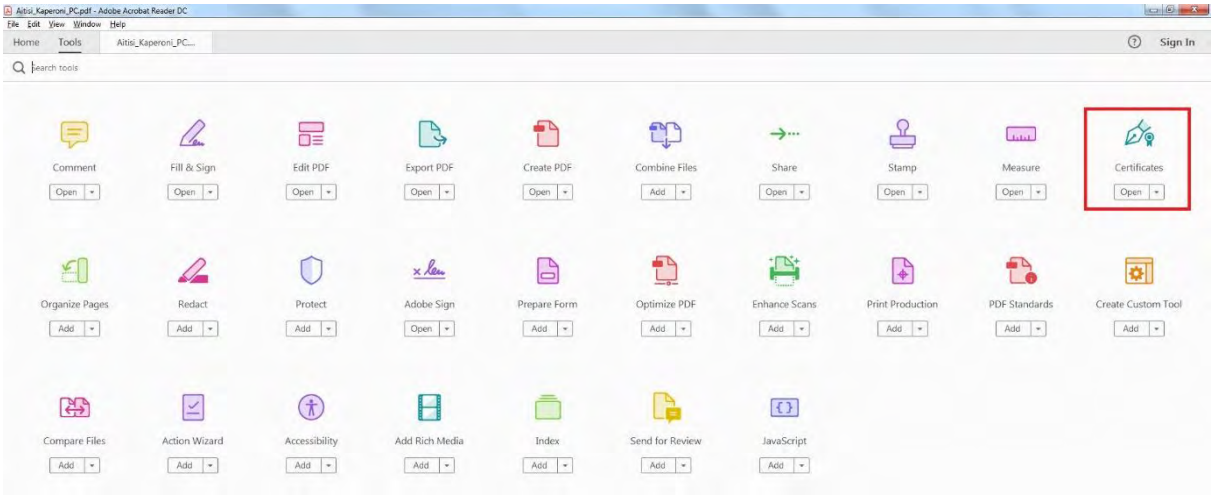


Εικόνα 65: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (6)

Βήμα 6ο:

Η επόμενη διαδικασία είναι η ψηφιακή υπογραφή αρχείου pdf με χρονοσήμανση.

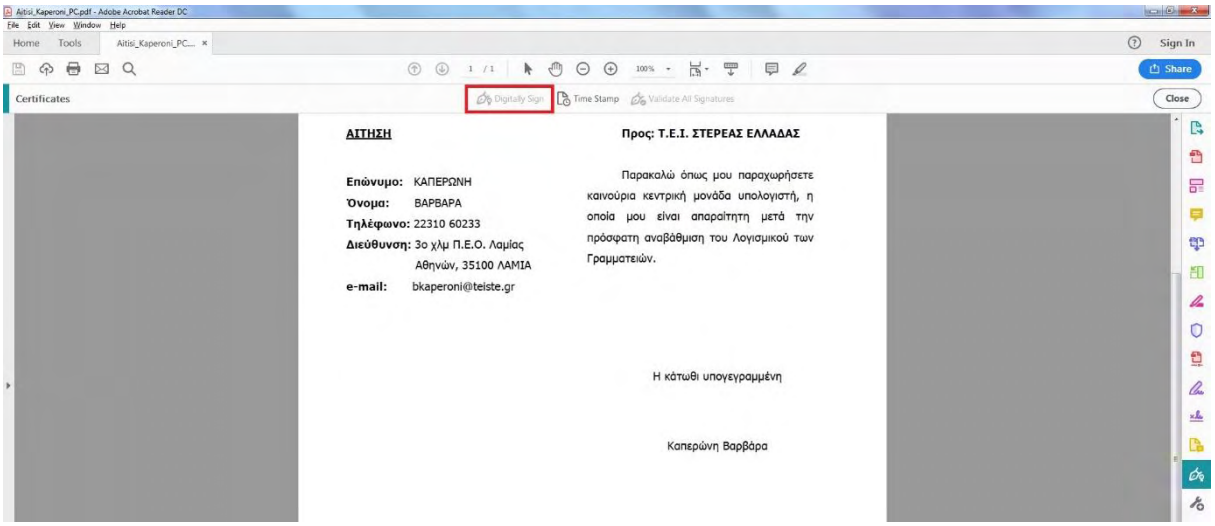
Έτσι, ανοίγουμε το pdf αρχείο που επιθυμούμε να υπογράψουμε ψηφιακά και επιλέγουμε **Tools -> Certificates.**



Εικόνα 66: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (7)

Βήμα 7ο:

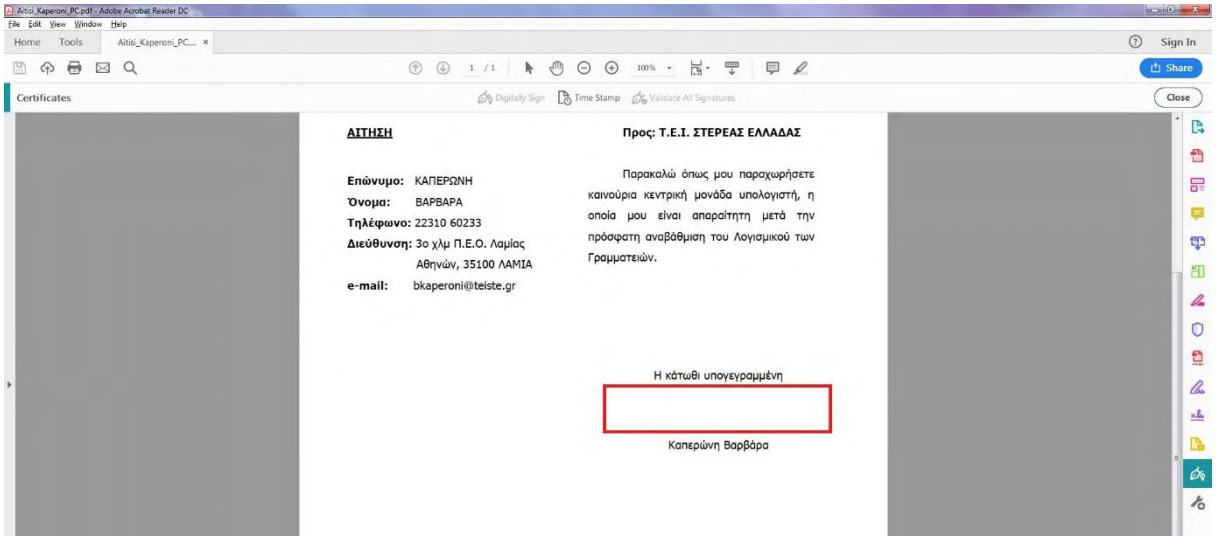
Επιλέγουμε **Digitally Sign -> OK**.



Εικόνα 67: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (8)

Βήμα 8ο:

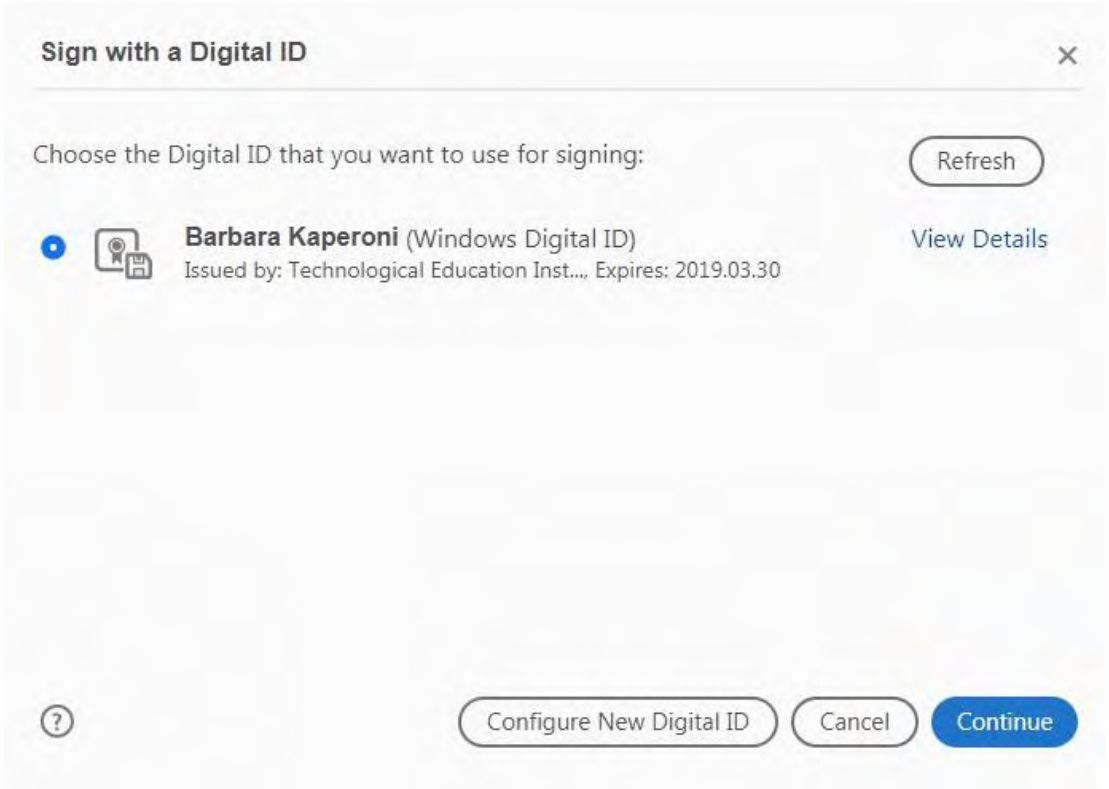
Σχεδιάζουμε ένα ορθογώνιο πλαίσιο μέσα στο οποίο θα εισάγουμε την ψηφιακή μας υπογραφή.



Εικόνα 68: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (9)

Βήμα 9ο:

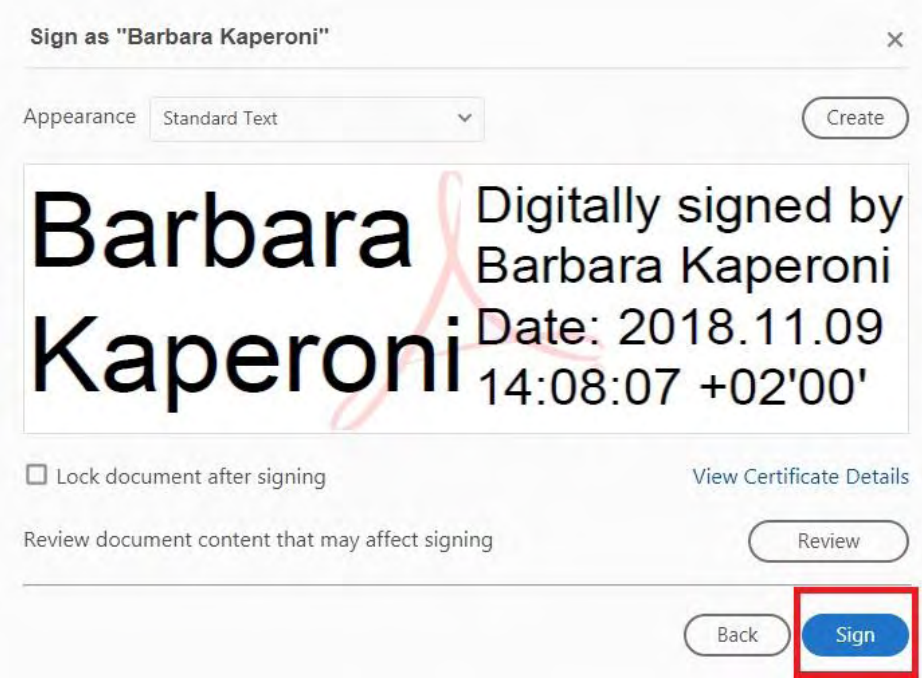
Ελέγχουμε εάν εμφανίζεται σωστά το πιστοποιητικό μας και επιλέγουμε **Continue.**



Εικόνα 69: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (10)

Βήμα 10ο:

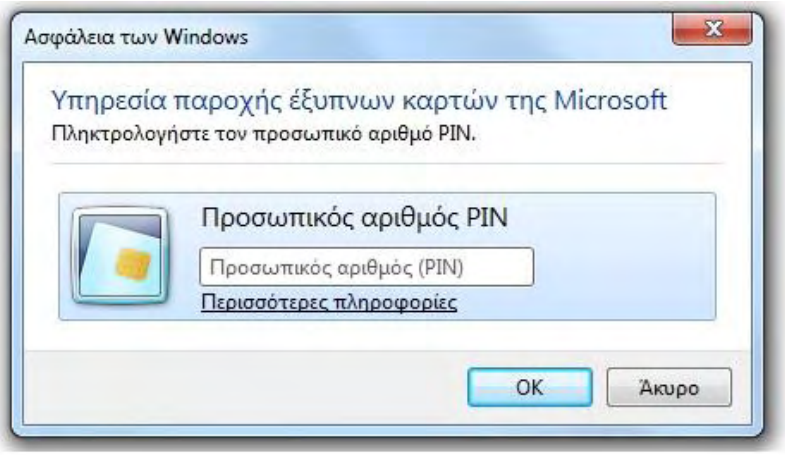
Στη συνέχεια επιλέγουμε **Sign**.



Εικόνα 70: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (11)

Βήμα 11ο:

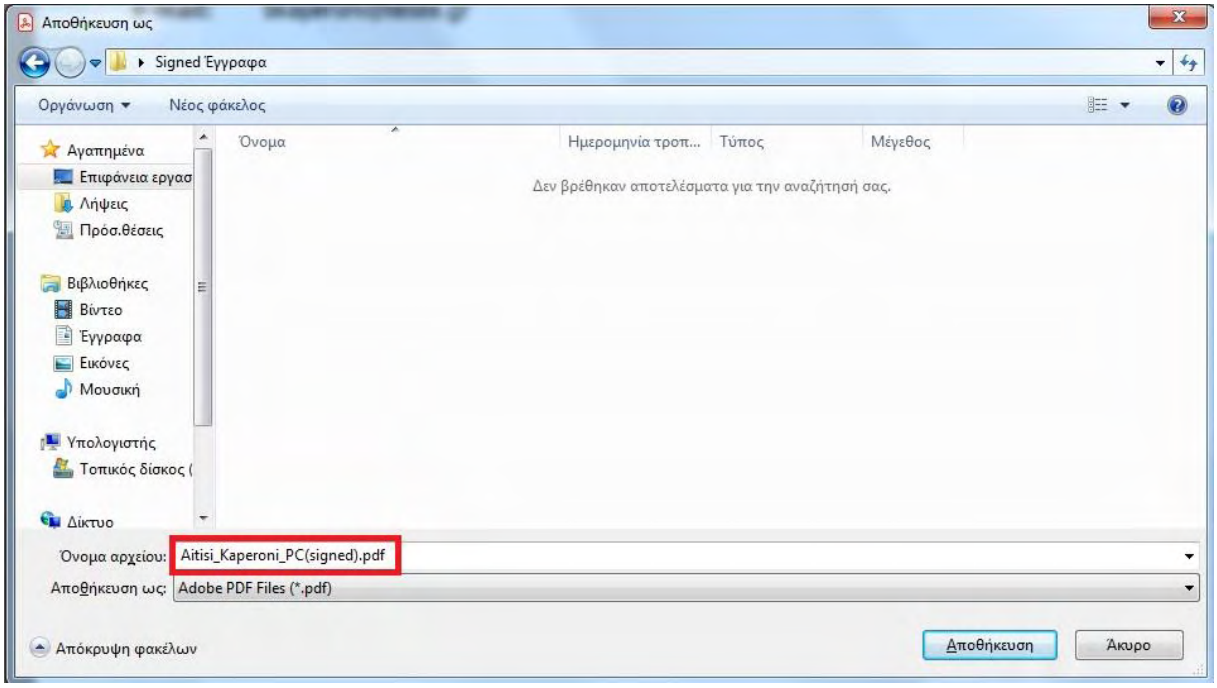
Για να ολοκληρωθεί η διαδικασία θα πρέπει να εισάγουμε το προσωπικό μας αριθμό (PIN).



Εικόνα 71: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (12)

Βήμα 12ο:

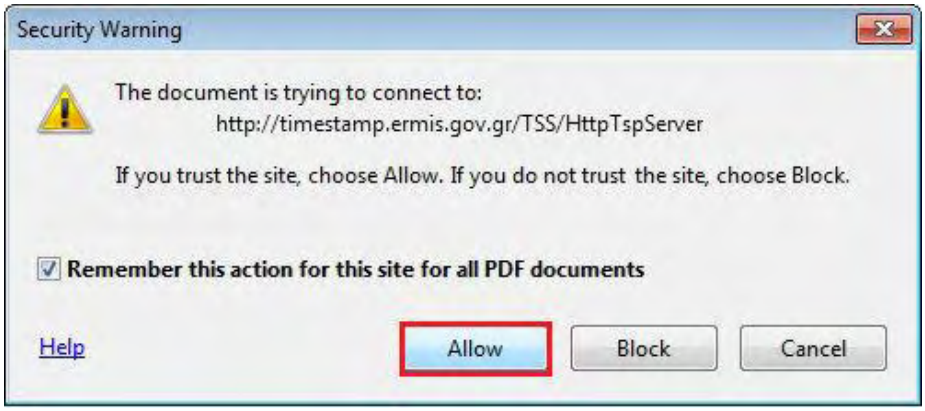
Το εισάγουμε και στη συνέχεια μας ζητείται να αποθηκεύσουμε το αρχείο μας.



Εικόνα 72: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (13)

Βήμα 13ο:

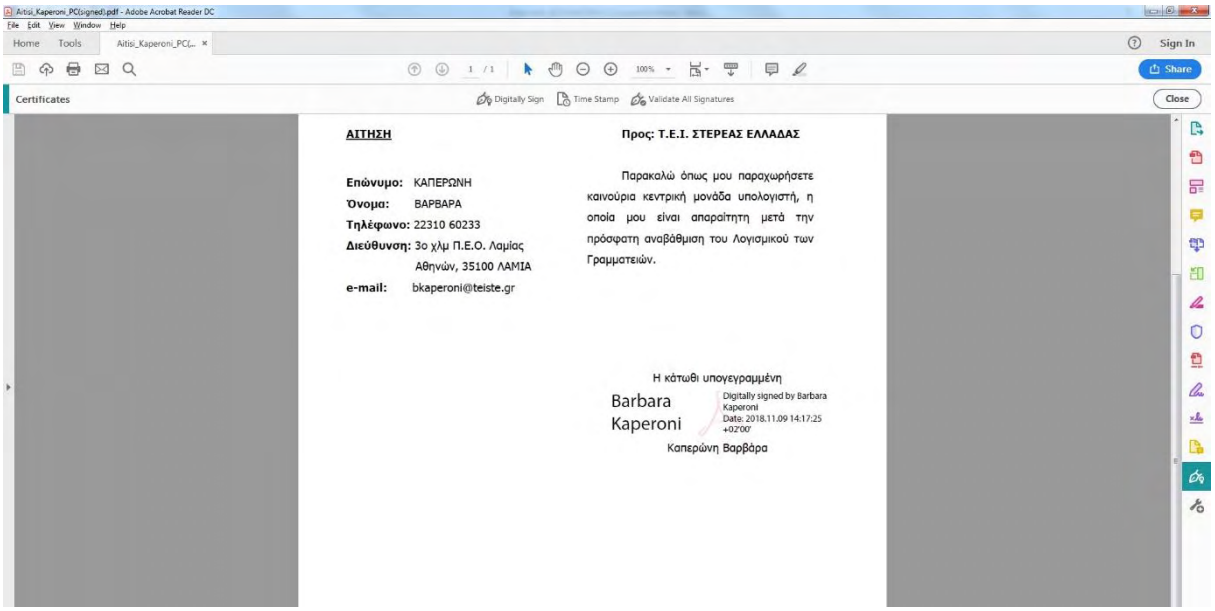
Στο μήνυμα σύνδεσης με το διακομιστή χρονοσήμανσης που ήδη έχουμε ορίσει, επιλέγουμε: **Να Επιτρέπεται / Allow**. Κάνουμε κλικ στο **Remember this action for this site for all PDF documents,** ούτως ώστε να αποθηκευτεί η επιλογή και να μην εμφανιστεί το μήνυμα αυτό την επόμενη φορά που θα υπογράψουμε ψηφιακά.



Εικόνα 73: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (14)

Βήμα 14ο:

Τέλος, το έγγραφό μας, όπως φαίνεται και παρακάτω, έχει υπογραφεί ψηφιακά με ημερομηνία και ώρα υπογραφής.



Εικόνα 74: Ρύθμιση Adobe Reader για χρήση ψηφιακής υπογραφής σε pdf αρχεία (15)

3.8. ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΜΗΝΥΜΑΤΟΣ ΜΕΣΩ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ΜΕ MOZILLA THUNDERBIRD

Μία άλλη διαδικασία που μπορούμε να χρησιμοποιήσουμε είναι η ψηφιακή υπογραφή μηνύματος μέσω ηλεκτρονικού ταχυδρομείου (e-mail). Μια ψηφιακή υπογραφή που έχει επισυναφθεί σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου προσφέρει ένα άλλο επίπεδο ασφαλείας, εξασφαλίζοντας στον παραλήπτη ότι εσύ ο αποστολέας (και όχι κάποιος που παριστάνει ότι είσαι εσύ), έχει υπογράψει τα περιεχόμενα του μηνύματος του ηλεκτρονικού ταχυδρομείου. Η ψηφιακή υπογραφή, η οποία περιλαμβάνει το πιστοποιητικό και το δημόσιο κλειδί, προέρχεται από την **ψηφιακή ταυτότητα (Digital ID)**. Με την ψηφιακή ταυτότητα επιτυγχάνεται επαλήθευση της αυθεντικότητας του αποστολέα, εξασφαλίζοντας επίσης στον

παραλήπτη ότι το περιεχόμενο του ηλεκτρονικού μηνύματος δεν έχει υποστεί τροποποίηση κατά τη μεταφορά βοηθώντας έτσι στην μη αλλοίωση των μηνυμάτων.

Για να ενσωματώσω την ψηφιακή υπογραφή μου (το προσωπικό μου ψηφιακό πιστοποιητικό) στην εφαρμογή ελεύθερου λογισμικού, παρακολούθησης ηλεκτρονικού ταχυδρομείου Mozilla Thunderbird (Ελληνική Έκδοση 60.2.1) θα ακολουθήσω την παρακάτω διαδικασία:

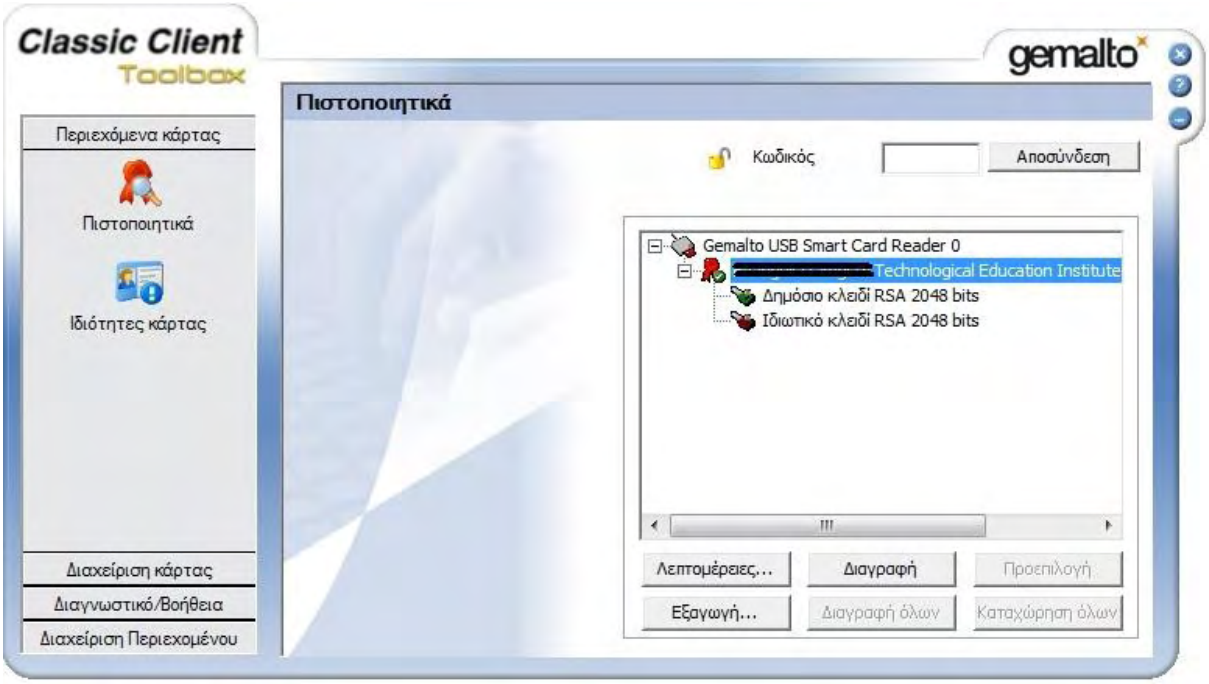
Σημείωση: Βασική προϋπόθεση είναι να υπάρχει το ψηφιακό μας πιστοποιητικό σε μορφή αρχείου, αποθηκευμένο στον υπολογιστή.

Βήμα 1ο:

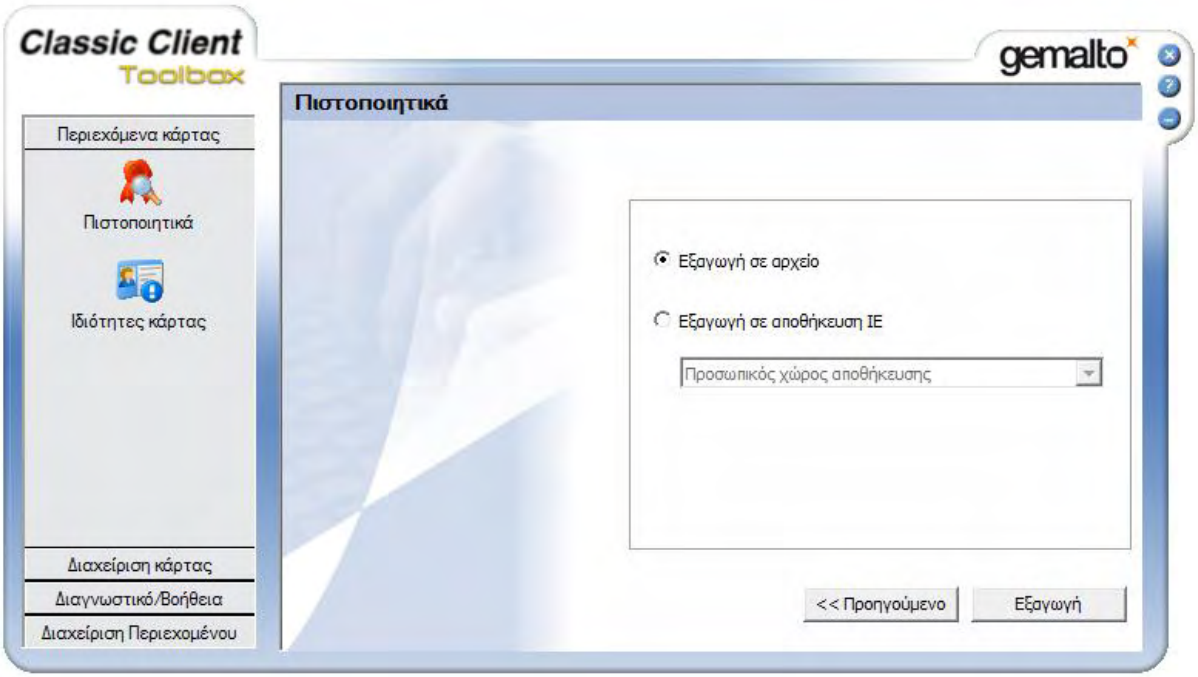
Αρχικά συνδέουμε τον αναγνώστη καρτών, έχοντας τοποθετήσει σε αυτόν την ακαδημαϊκή μας ταυτότητα. Επιλέγω το προσωπικό πιστοποιητικό του χρήστη και επιλέγω **«Εξαγωγή»**.

Βήμα 2ο:

Επιλέγουμε **«Εξαγωγή σε αρχείο»** και **«Εξαγωγή»**.



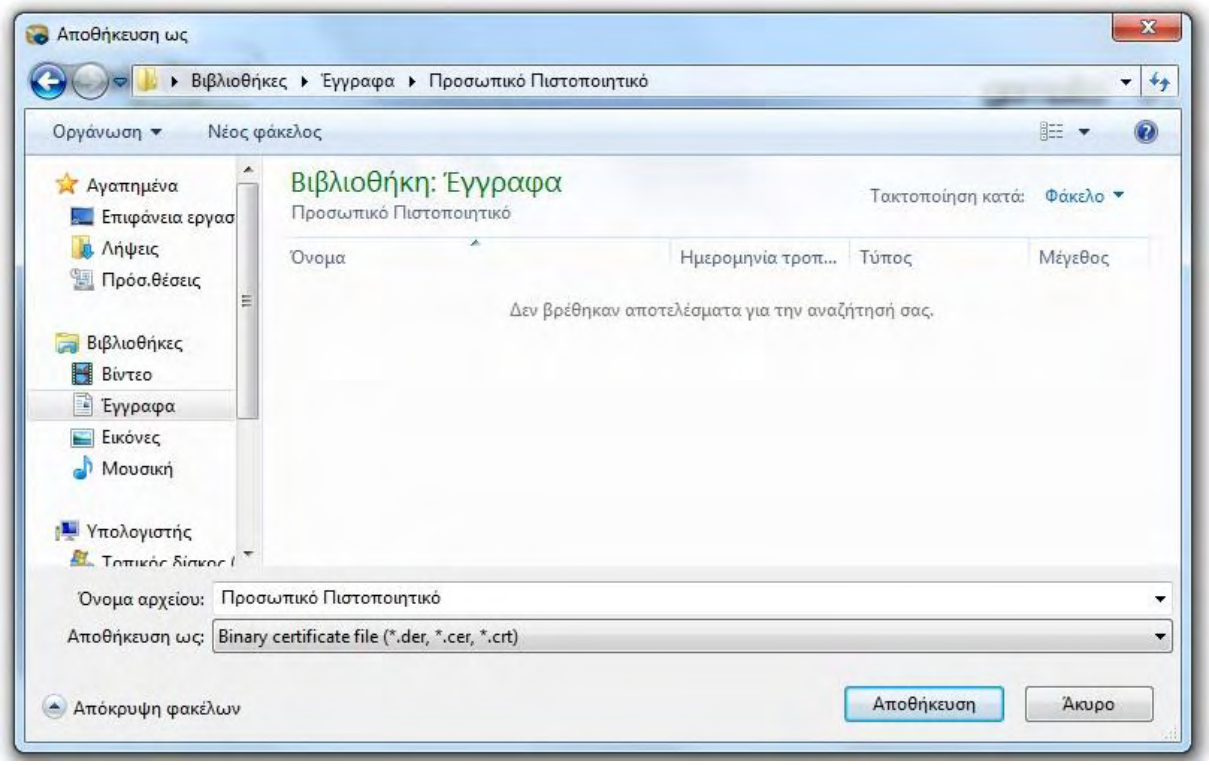
Εικόνα 75: Εξαγωγή ψηφιακού πιστοποιητικού από την ακαδημαϊκή ταυτότητα (1)



Εικόνα 76: Εξαγωγή ψηφιακού πιστοποιητικού από την ακαδημαϊκή ταυτότητα (2)

Βήμα 3ο:

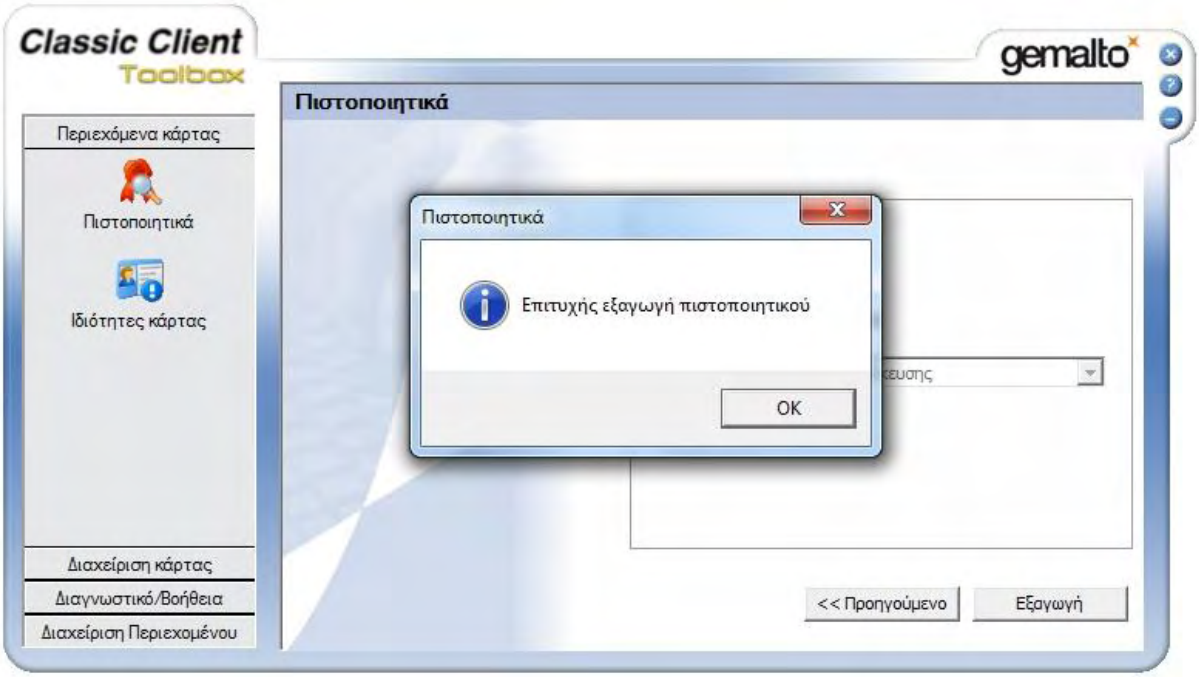
Επιλέγουμε τον φάκελο που θα το αποθηκεύσουμε και το όνομα με το οποίο θα το αποθηκεύσουμε και κάνουμε κλικ στο «**Αποθήκευση**».



Εικόνα 77: Εξαγωγή ψηφιακού πιστοποιητικού από την ακαδημαϊκή ταυτότητα (3)

Βήμα 4ο:

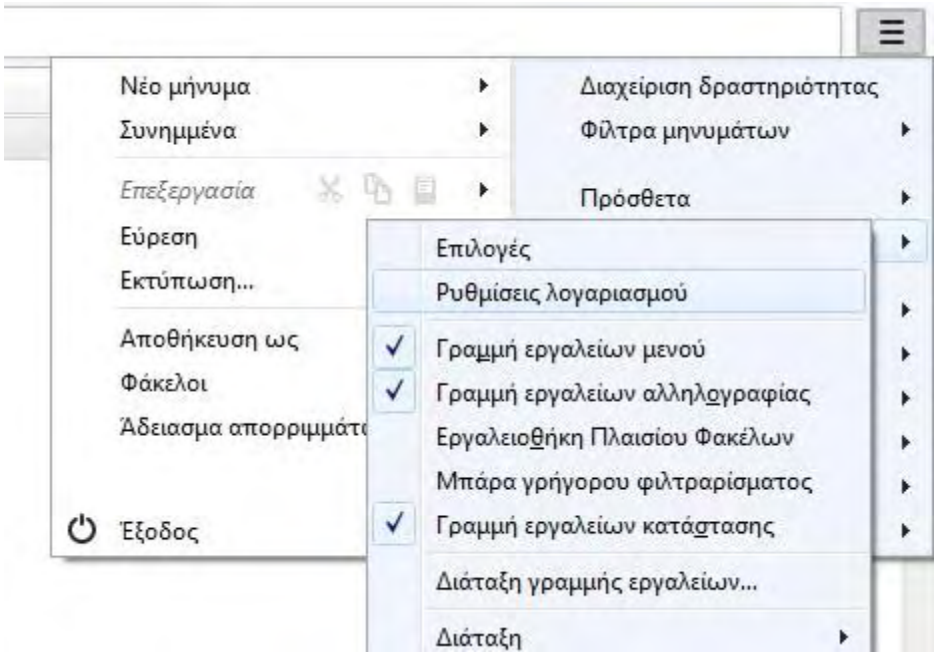
Μόλις εξαχθεί, θα μας βγάλει το παρακάτω μήνυμα **«Επιτυχής εξαγωγή πιστοποιητικού»**.



Εικόνα 78: Εξαγωγή ψηφιακού πιστοποιητικού από την ακαδημαϊκή ταυτότητα (4)

Βήμα 5ο:

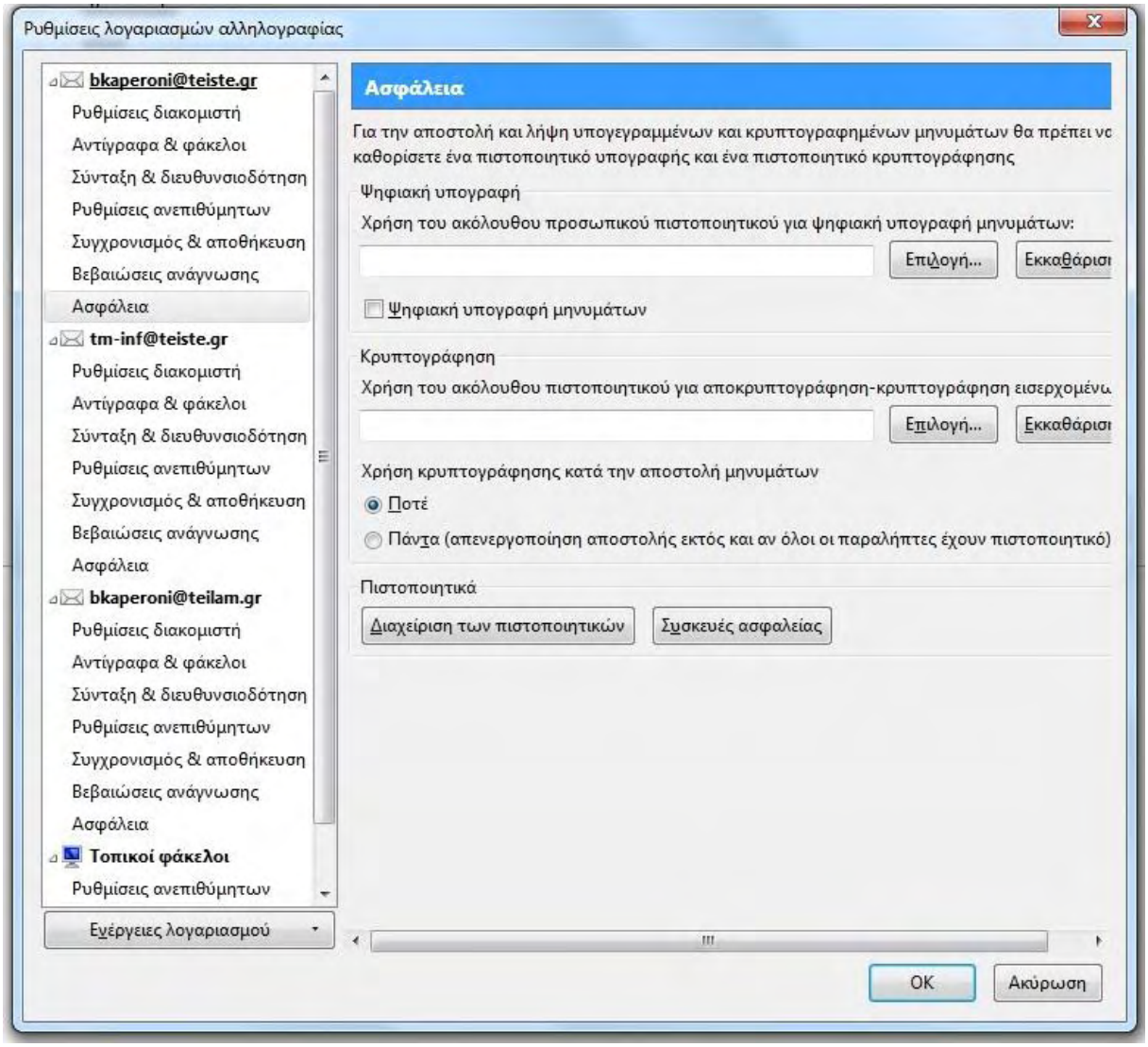
Στο δεξί μέρος του Μενού του Mozilla Thunderbird (Τρεις γραμμές), κάνουμε κλικ στο **«Επιλογές» και έπειτα «Ρυθμίσεις Λογαριασμού»**.



Εικόνα 79: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (1)

Βήμα 6ο:

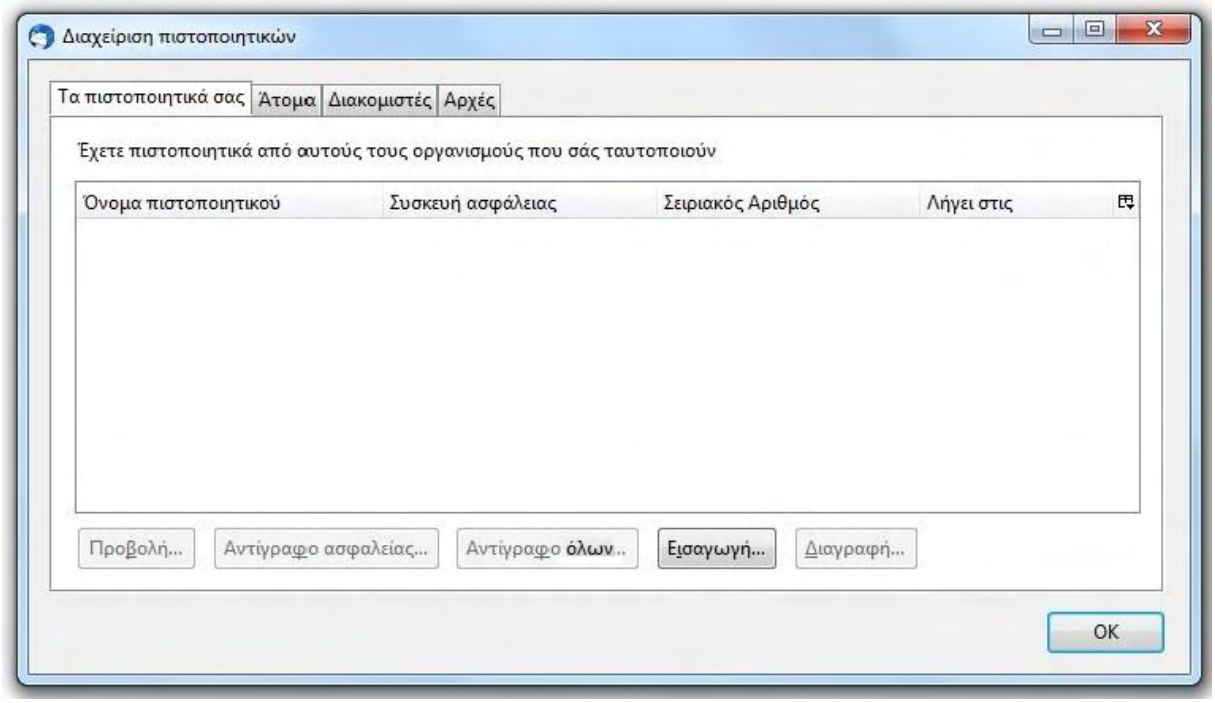
Στην καρτέλα «Ασφάλεια» επιλέγουμε «Διαχείριση των Πιστοποιητικών».



Εικόνα 80: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (2)

Βήμα 7ο:

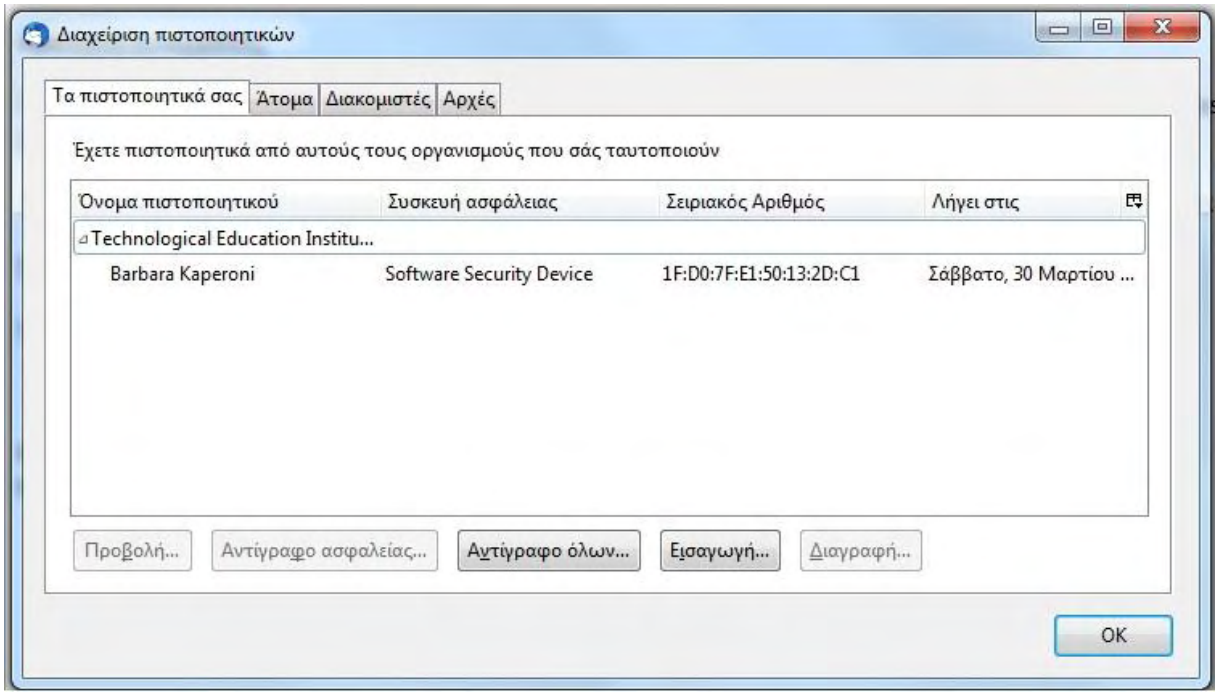
Από την καρτέλα «**Τα Πιστοποιητικά σας**» επιλέγουμε «**Εισαγωγή**». Αναζητούμε το αρχείο του πιστοποιητικού μας, όπου το έχουμε αποθηκεύσει, και κάνουμε κλικ στο «**Άνοιγμα**».



Εικόνα 81: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (3)

Βήμα 8ο:

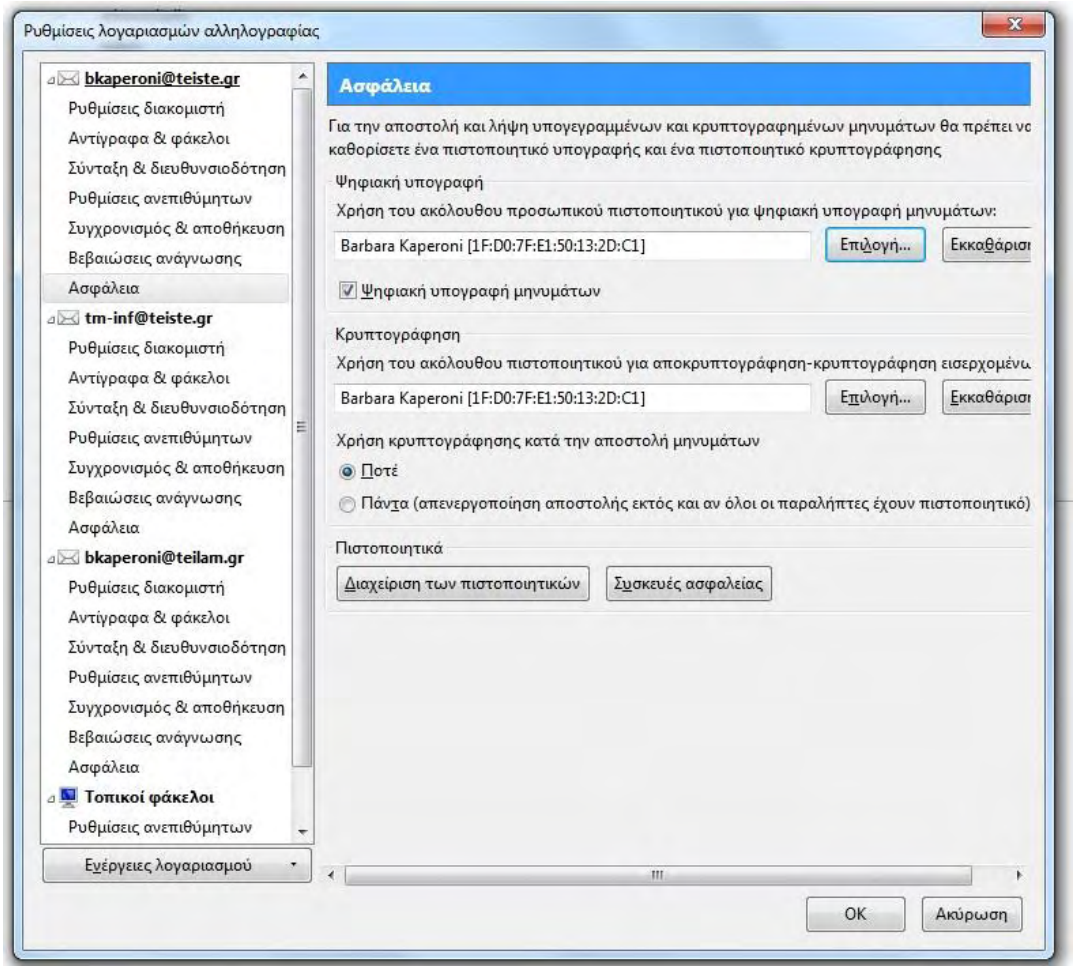
Στη συνέχεια εμφανίζεται το πιστοποιητικό μας και επιλέγουμε οκ.



Εικόνα 82: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (4)

Βήμα 9ο:

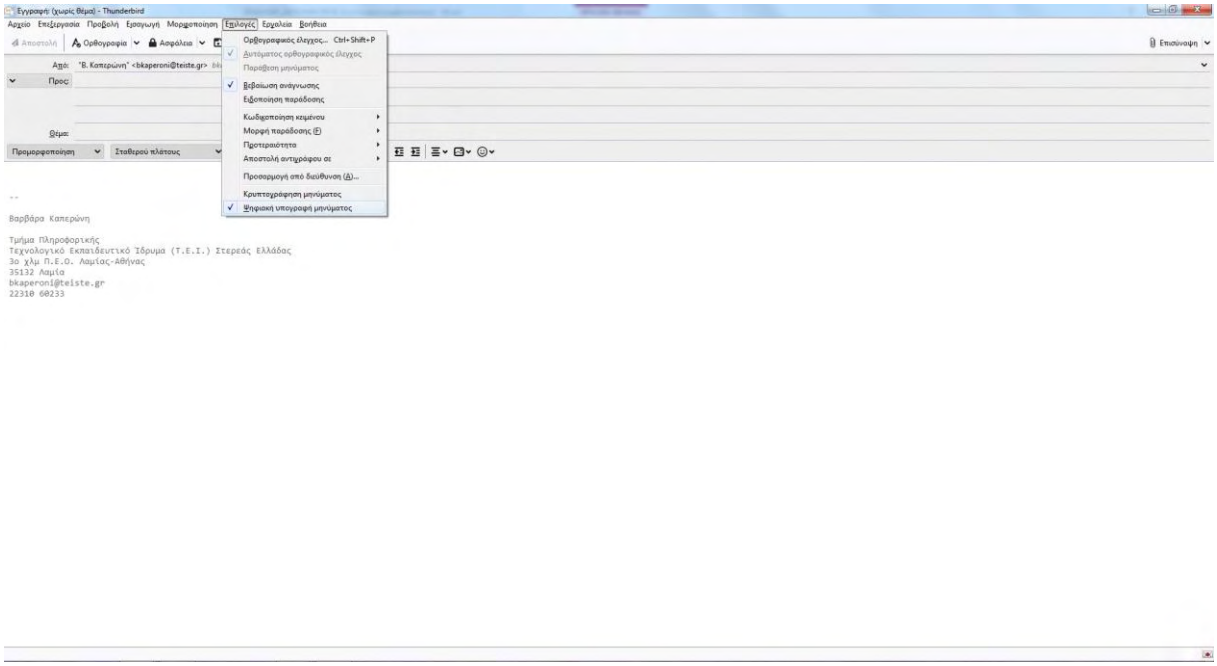
Από την καρτέλα «Ασφάλεια» και στο «Ψηφιακή Υπογραφή» κάνουμε κλικ στο «Επιλογή». Επιλέγουμε το πιστοποιητικό μας και πατάμε OK. Για να ορίσουμε το ίδιο πιστοποιητικό να χρησιμοποιείται και στην περίπτωση κρυπτογράφησης, πατάμε Ναι στην ερώτηση. Τέλος, κάνουμε κλικ στο **«Ψηφιακή υπογραφή μηνυμάτων»**, εάν επιθυμούμε όλα τα μηνύματα να υπογράφονται ψηφιακά και κάνουμε κλικ στο OK.



Εικόνα 83: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (5)

Βήμα 10ο:

Κατά την δημιουργία μηνύματος, επιλέγουμε Ρυθμίσεις -> «Ψηφιακή υπογραφή μηνύματος». Καταλαβαίνουμε ότι το μήνυμα ηλεκτρονικού ταχυδρομείου το συνοδεύει μία ψηφιακή υπογραφή, από την ένδειξη του εικονιδίου του φακέλου στο παράθυρο κάτω δεξιά.



Εικόνα 84: Ρύθμιση Mozilla Thunderbird για ψηφιακή υπογραφή μηνυμάτων (6)

ΚΕΦΑΛΑΙΟ 4: ΣΥΣΤΗΜΑ ΕΚΔΟΣΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΓΡΑΦΗΣ ΜΕΣΩ ΤΗΣ ΠΥΛΗΣ ΕΡΜΗΣ

4.1. ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό θα δούμε πληροφορίες σχετικά με την πύλη ΕΡΜΗΣ και θα περιγράψουμε τα βήματα για την διαδικασία της ηλεκτρονικής υποβολής αιτήματος έκδοσης ψηφιακών πιστοποιητικών μέσω της πύλης ΕΡΜΗΣ.

4.2. ΟΡΙΣΜΟΣ ΤΗΣ ΠΥΛΗΣ ΕΡΜΗΣ

Η Εθνική Πύλη Δημόσιας Διοίκησης ΕΡΜΗΣ[23] «Ermis», αποτελεί το εμπνευσμένο πρόγραμμα της Ελληνικής Κυβέρνησης, προς την κατεύθυνση της πληροφόρησης των πολιτών αλλά και των επιχειρήσεων, για την ασφαλή διεκπεραίωση υπηρεσιών ηλεκτρονικής διακυβέρνησης.

Απώτερος σκοπός της κυβερνητικής Διαδικτυακής Πύλης ΕΡΜΗΣ είναι ο εκσυγχρονισμός της Δημόσιας Διοίκησης μέσα από μία σειρά υπηρεσιών ηλεκτρονικών συναλλαγών που παρέχονται για την εξυπηρέτηση των πολιτών. Από τις 9 Νοεμβρίου 2015, μέσω των ηλεκτρονικών κωδικών του **TAXISnet,** οι πολίτες μπορούν να έχουν πρόσβαση σε υπηρεσίες που προσφέρει η πύλη ΕΡΜΗΣ, χωρίς να είναι απαραίτητη η φυσική τους παρουσία σε Κέντρα Εξυπηρέτησης Πολιτών (Κ.Ε.Π.). Οι πιο σημαντικές υπηρεσίες είναι:

- Χορήγηση πιστοποιητικού γέννησης
- Χορήγηση βεβαίωσης οικογενειακής κατάστασης
- Χορήγηση αντιγράφου ληξιαρχικής πράξης γάμου
- Χορήγηση βεβαίωσης ιθαγένειας
- Χορήγηση αντιγράφου ληξιαρχικής πράξης θανάτου
- Απόσπασμα ατομικού λογαριασμού ΙΚΑ
- Δυνατότητα απόκτησης ψηφιακής υπογραφής, μέσω έκδοσης προσωπικού ψηφιακού πιστοποιητικού.

[23] www.ermis.gov.gr

Κάθε πολίτης διαθέτει μία προσωπική ηλεκτρονική θυρίδα. Όταν αιτείται για κάποια από τις υπηρεσίες του ΕΡΜΗ, το αποτέλεσμα της αίτησής του (βεβαίωση, πιστοποιητικό) μπορεί να το παραλάβει στην θυρίδα αυτή, όπου το αποθηκεύει ή/και το εκτυπώνει (ψηφιοποίηση εγγράφων). Έχει επίσης την δυνατότητα να το παραλάβει από ένα ΚΕΠ, δηλώνοντάς την επιθυμία του κατά την υποβολή της αίτησης.

Τα ηλεκτρονικά έγγραφα που προκύπτουν από την συγκεκριμένη διαδικασία έχουν ένα μοναδικό κωδικό, τον «Κωδικό Επαλήθευσης» έτσι ώστε να είναι έγκυρα κάθε στιγμή.

4.3. ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΒΟΛΗ ΑΙΤΗΜΑΤΟΣ ΕΚΔΟΣΗΣ ΨΗΦΙΑΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΜΕΣΩ ΤΗΣ ΠΥΛΗΣ ΕΡΜΗΣ

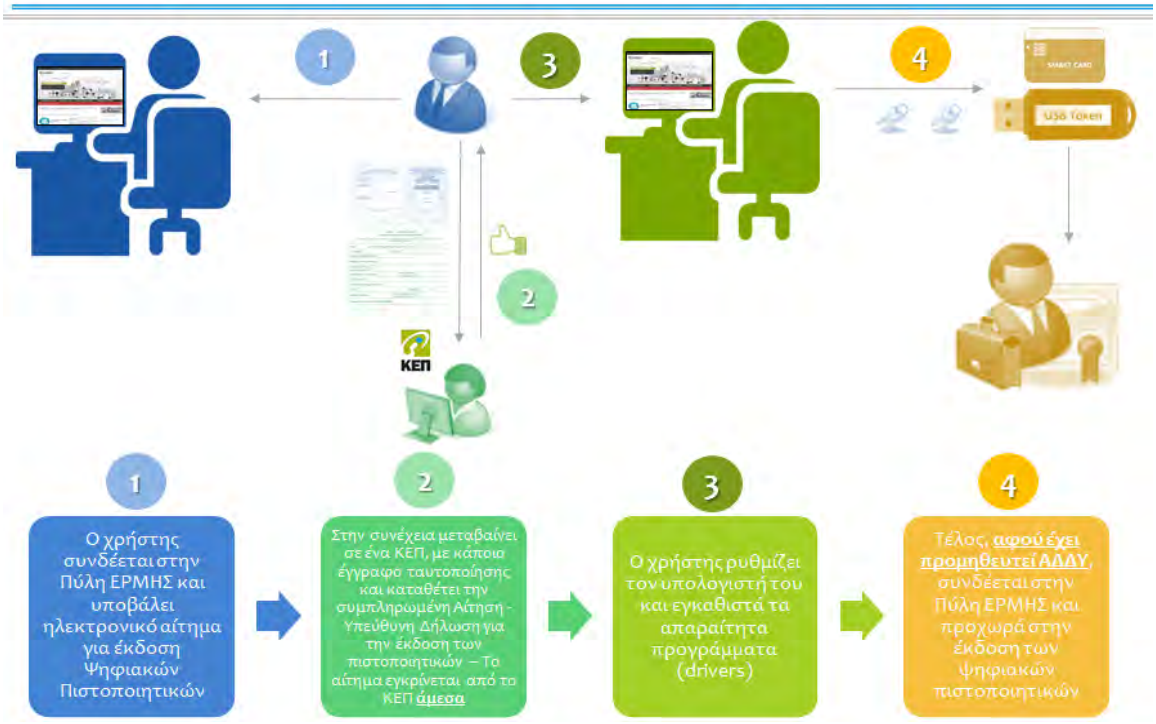
Στην ενότητα αυτή θα περιγράψουμε την διαδικασία ηλεκτρονική υποβολή αιτήματος έκδοσης ψηφιακών πιστοποιητικών μέσω της πύλης ΕΡΜΗΣ. Η πύλη ΕΡΜΗΣ ως Πρωτεύουσα Αρχή Πιστοποίησης» (ΠΑΠ), χρησιμοποιεί την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)[24].

Μέσω της ΑΠΕΔ, ο πολίτης έχει την δυνατότητα έκδοσης προσωπικών ψηφιακών πιστοποιητικών που χρησιμοποιούνται για αυθεντικοποίηση, κρυπτογράφηση και ψηφιακή υπογραφή, καθιστώντας τις ηλεκτρονικές συναλλαγές τους πιο ασφαλείς.

Στην περίπτωση ειδικά των δημοσίων υπαλλήλων, η διαδικασία έκδοσης προσωπικών ψηφιακών πιστοποιητικών και απόκτησης ψηφιακής υπογραφής είναι υποχρεωτική σε αρκετές διαδικασίες, όπως η διακίνηση εγγράφων με θέση ευθύνης (προϊσταμένου-ης, διευθυντή-τριας), η συμμετοχή τους σε επιτροπές ηλεκτρονικών διαγωνισμών κλπ.

Στην παρακάτω εικόνα περιγράφεται συνοπτικά η διαδικασία έκδοσης ψηφιακών πιστοποιητικών μέσω της πύλης ΕΡΜΗΣ:

[24] http://www.aped.gov.gr



Εικόνα 85: Συνοπτική περιγραφή διαδικασίας έκδοσης ψηφιακών πιστοποιητικών

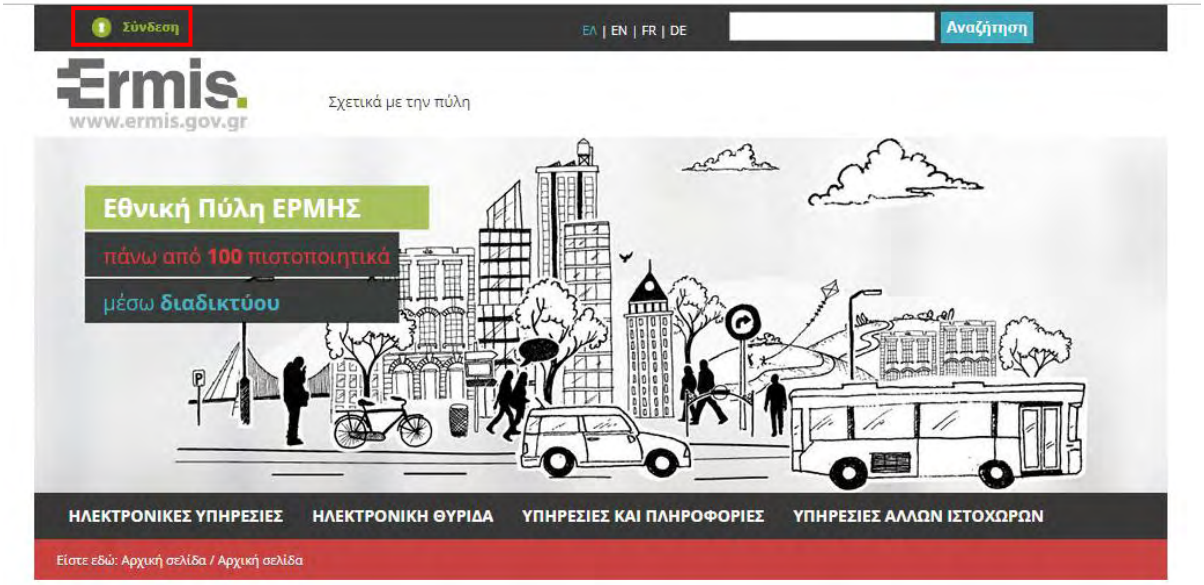
Μέχρι τις 19 Ιουνίου 2018, τα ψηφιακά πιστοποιητικά που είχαν εκδοθεί από την ΑΠΕΔ είχαν διάρκεια ισχύος πέντε (5) χρόνια. Από τις 20 Ιουνίου 2018, τα πιστοποιητικά που εκδίδονται έχουν διάρκεια ισχύος τα τρία 3 χρόνια.

Στη συνέχεια περιγράφεται αναλυτικά η πρωταρχική διαδικασία που πρέπει να ακολουθηθεί προκειμένου να υποβληθεί ηλεκτρονικό αίτημα έκδοσης ψηφιακών πιστοποιητικών[25].

Βήμα 1ο: Σύνδεση στη Πύλη ΕΡΜΗΣ

Αρχικά, μεταβαίνουμε στο σύνδεσμο http://www.ermis.gov.gr/portal/page/portal/ermis/ και επιλέγουμε τον σύνδεσμο ***Σύνδεση*** όπως διακρίνεται με κόκκινο πλαίσιο στην παρακάτω εικόνα:

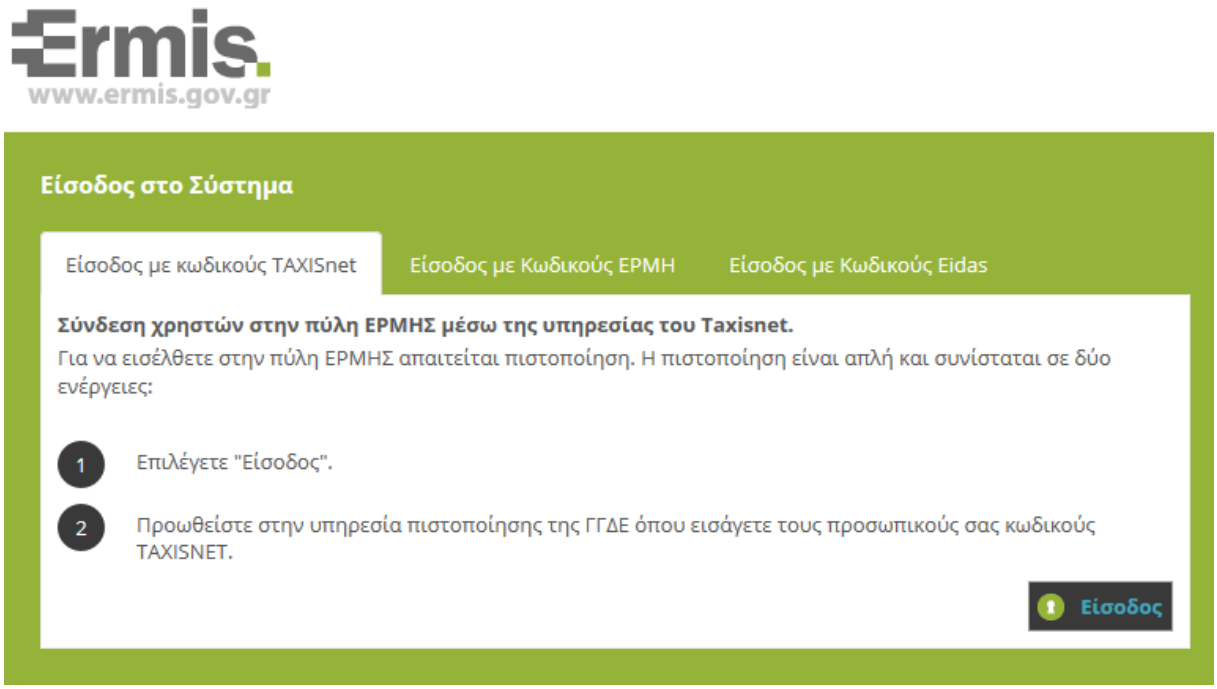
[25]http://www.aped.gov.gr/images/steps1-6/step_2_submit_application_for_pki_certificates_v2_2.pdf



Εικόνα 86: Σύνδεση στη Πύλη ΕΡΜΗΣ

Βήμα 2ο:

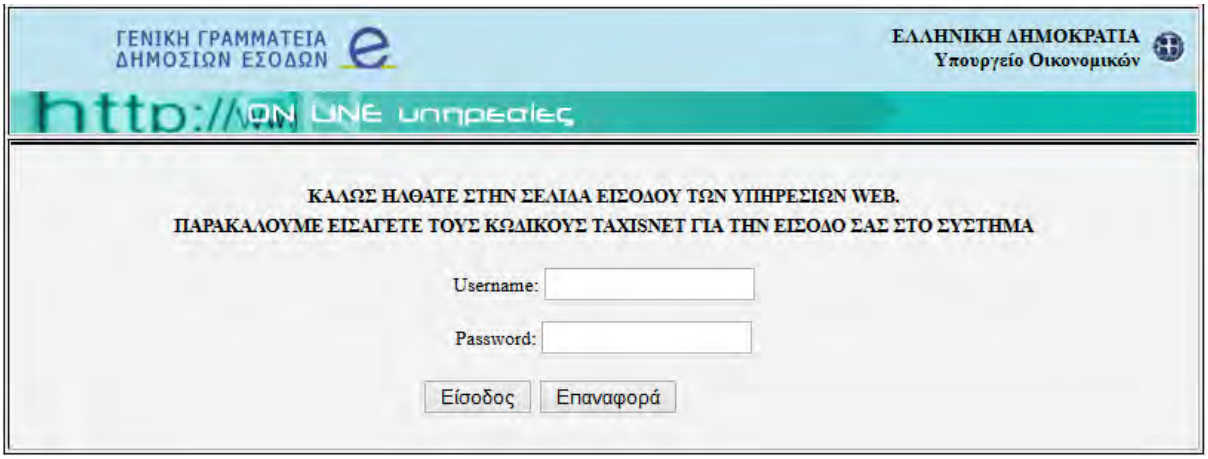
Στη συνέχεια επιλέγουμε τον σύνδεσμο ***Είσοδος,*** οπότε εμφανίζεται η παρακάτω εικόνα:



Εικόνα 87: Είσοδος στην Πύλη ΕΡΜΗΣ

Βήμα 3ο:

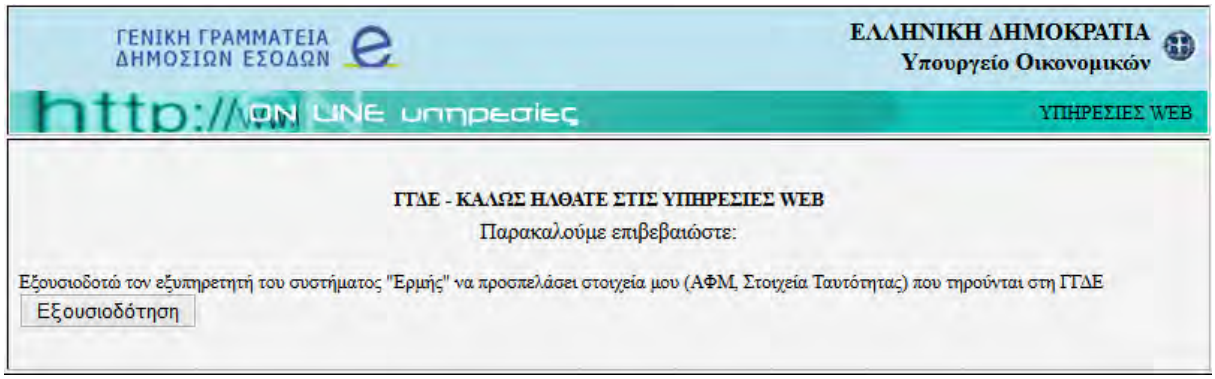
Κατόπιν, πληκτρολογούμε τους προσωπικούς κωδικούς του TAXISnet:



Εικόνα 88: Οθόνη εισαγωγής κωδικών

Βήμα 4ο:

Στην συνέχεια επιλέγουμε «Εξουσιοδότηση» και μεταφερόμαστε στην αρχική σελίδα της εφαρμογής.

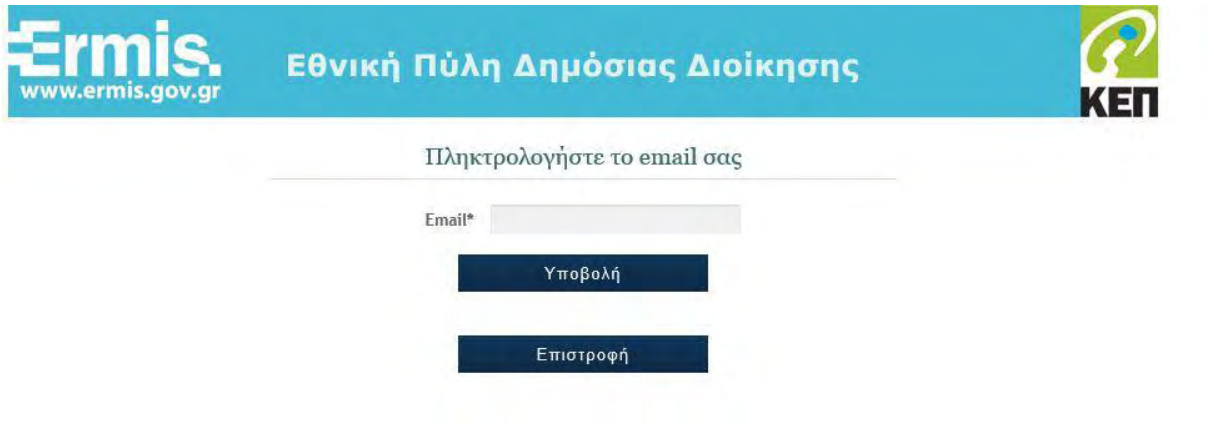


Εικόνα 89: Εξουσιοδότηση

Σημείωση: Με την επιλογή της «Εξουσιοδότησης», εξουσιοδοτούμε τον εξυπηρετητή του Συστήματος ΕΡΜΗΣ να προσπελάσει τα στοιχεία μας, όπως το ΑΦΜ, τα στοιχεία της ταυτότητάς μας, που ήδη τηρούνται στην εφαρμογή της ΓΓΔΕ (Γενική Γραμματεία Δημοσίων Εσόδων).

Βήμα 5ο:

Όταν είναι η πρώτη φορά που εισερχόμαστε στην Πύλη ΕΡΜΗΣ, θα πρέπει να πληκτρολογήσουμε μια ηλεκτρονική διεύθυνση (e-mail) και στη συνέχεια να κάνουμε κλικ στο ***Υποβολή***.



Εικόνα 90: Συμπλήρωση email

Βήμα 6ο:

Με την ολοκλήρωση της παραπάνω διαδικασίας, μεταφερόμαστε στην κεντρική σελίδα της Πύλης ΕΡΜΗΣ, όπου έχει ήδη δημιουργηθεί ο καινούργιος λογαριασμός.

Ο λογαριασμός αυτός περιλαμβάνει για κάθε χρήστη ένα όνομα χρήστη (username) το οποίο είναι της μορφής «**Ermis_αριθμός**», όπως φαίνεται με κόκκινο πλαίσιο στην Εικόνα 91. Το username αυτό πρέπει να το αποθηκεύσουμε και να το συμπληρώσουμε στην έντυπη *Αίτηση – Υπεύθυνη Δήλωση έκδοσης ψηφιακών πιστοποιητικών*[26] που απαιτείται να προσκομίσουμε σε ένα ΚΕΠ, έτσι ώστε να ολοκληρωθεί το Βήμα 3ο της διαδικασίας απόκτησης ψηφιακής υπογραφής - Εικόνα 85).

[26] http://www.aped.gov.gr/images/entypa/pki_citizen_yp_dilosi.pdf

Εικόνα 91: Όνομα χρήστη πύλης ΕΡΜΗΣ

Βήμα 7ο: Υποβολή Αιτήματος Έκδοσης Ψηφιακού Πιστοποιητικού

Εφόσον, είμαστε συνδεδεμένοι στην Πύλη ΕΡΜΗΣ, προχωράμε στην υποβολή αιτήματος έκδοσης Ψηφιακού Πιστοποιητικού από την ΑΠΕΔ. Έτσι, μεταβαίνουμε στο μενού **«Λειτουργίες της πύλης»** και επιλέγουμε τον σύνδεσμο **«Πίνακας Ελέγχου»**, όπως φαίνεται με κόκκινο πλαίσιο στην παρακάτω εικόνα :

Εικόνα 92: Πίνακας Ελέγχου πύλης ΕΡΜΗΣ

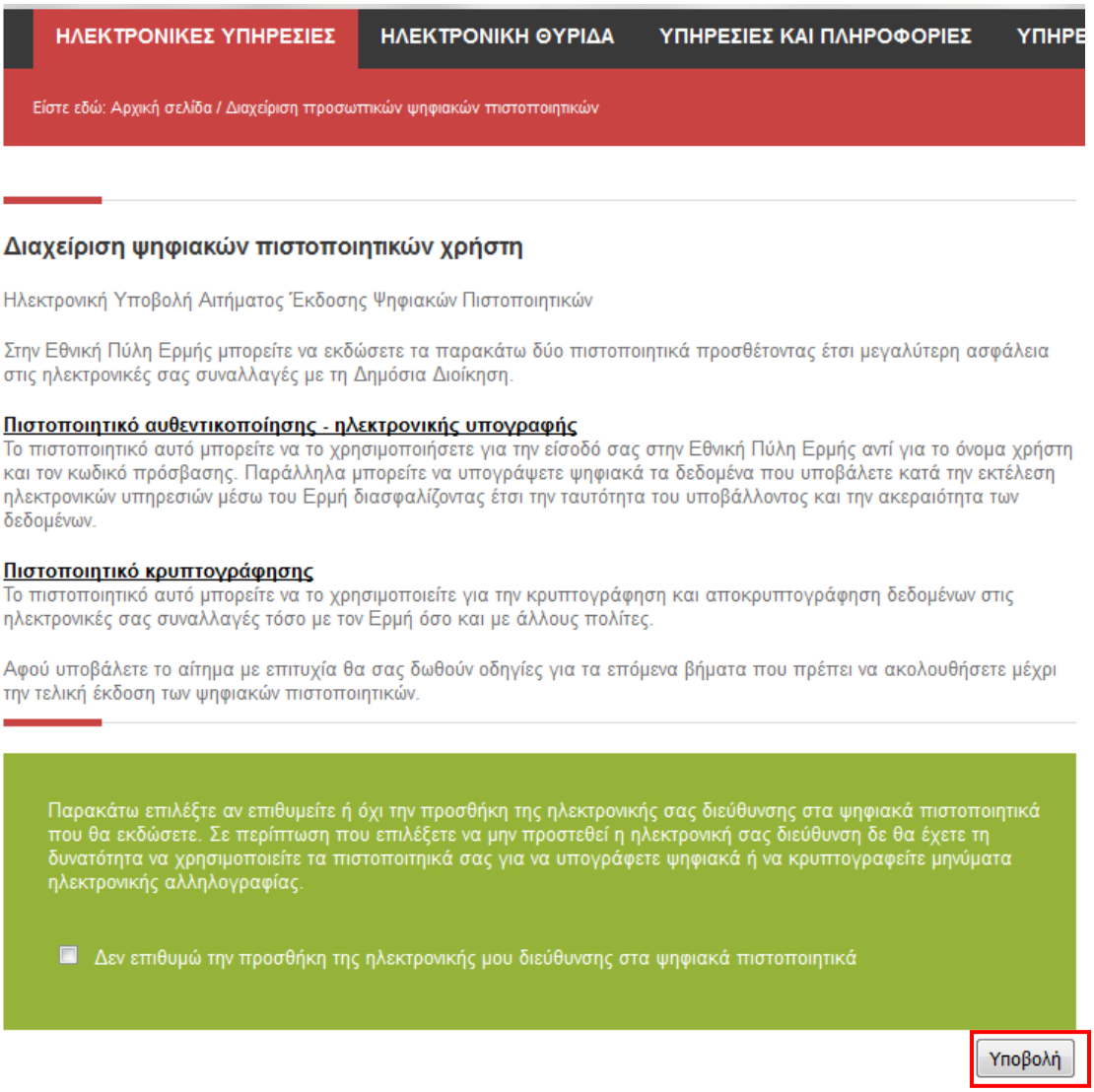
Βήμα 8ο:

Εμφανίζεται ο Πίνακας Ελέγχου του Χρήστη, όπου επιλέγουμε τον σύνδεσμο «**Διαχείριση Προσωπικών Ψηφιακών Πιστοποιητικών**».

Εικόνα 93: Πίνακας Ελέγχου - Διαχείριση προσωπικών ψηφιακών πιστοποιητικών

Βήμα 9ο:

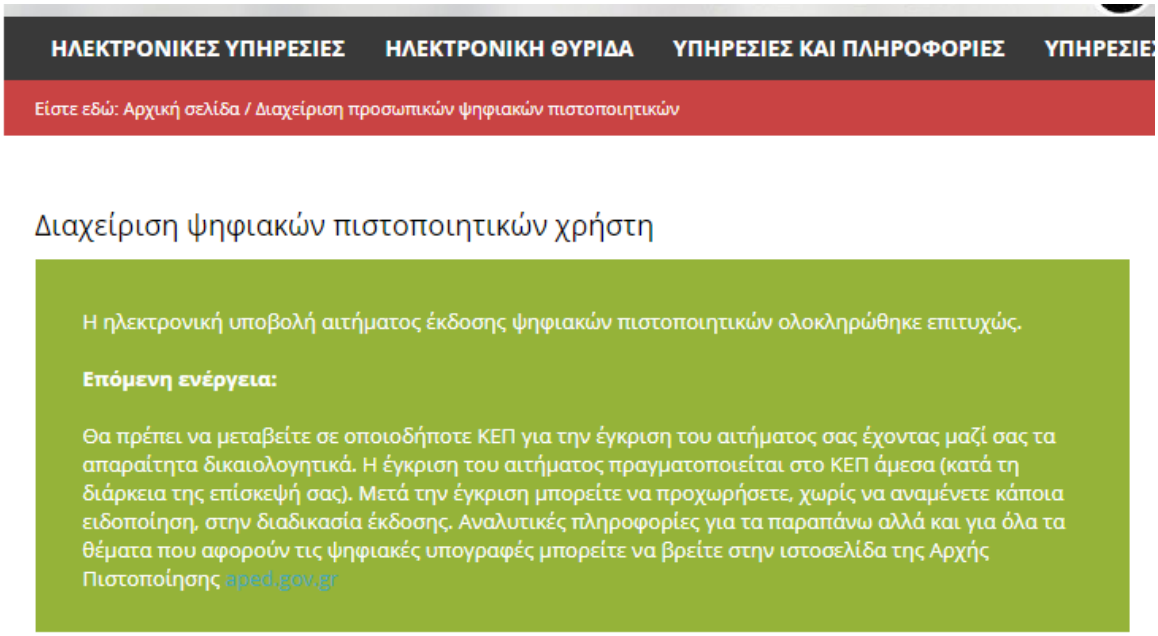
Στη συνέχεια, εμφανίζεται η δυνατότητα ηλεκτρονικής υποβολής αιτήματος έκδοσης ψηφιακού πιστοποιητικού:



Εικόνα 94: Ηλεκτρονική Υποβολή Αιτήματος Έκδοσης Ψηφιακών Πιστοποιητικών

Βήμα 10ο:

Κάνουμε κλικ στο κουμπί «**Υποβολή**» και εμφανίζεται το ακόλουθο μήνυμα την επιτυχούς ολοκλήρωσης της διαδικασίας. Στην συνέχεια, θα πρέπει να επισκεφτούμε ένα Κέντρο Εξυπηρέτησης Πολιτών (ΚΕΠ) για την έγκριση του αιτήματος μας:



Εικόνα 95: Ολοκλήρωση Υποβολής Αιτήματος Έκδοσης Ψηφιακών Πιστοποιητικών

Βήμα 11ο:

Εφόσον έχει ολοκληρωθεί από το ΚΕΠ η έγκριση του αιτήματος μας, θα πρέπει να προχωρήσουμε στο τελικό στάδιο της έκδοσης και εγκατάσταση ψηφιακών πιστοποιητικών σκληρής αποθήκευσης.

Το εγχειρίδιο οδηγιών[27], όπως αναφέρεται τον παρακάτω σύνδεσμο, περιγράφει αναλυτικά το σύνολο των βημάτων που απαιτούνται για την ολοκλήρωση της διαδικασίας αυτής.

[27] http://www.ermis.gov.gr/portal/page/portal/ermis/items/pdfs/pkiguide_hw.pdf

ΚΕΦΑΛΑΙΟ 5: ΜΗΤΡΩΟ ΠΟΛΙΤΩΝ ΚΑΙ ΚΑΡΤΑ ΠΟΛΙΤΗ

5.1. ΕΙΣΑΓΩΓΗ

Παρόλο που η διαδικασία της ηλεκτρονική υπογραφής ξεκίνησε να υλοποιείται, εντούτοις πολλοί χρήστες, έδειξαν να εγκαταλείπουν την προσπάθεια για την απόκτηση της Ψηφιακής Υπογραφής λόγω δυσκολιών στην εφαρμογή των οδηγιών της.

Κατά συνέπεια, λαμβάνοντας υπόψιν τη σημερινή κατάσταση, ο πολίτης έρχεται ακόμη αντιμέτωπος με γραφειοκρατικές και χρονοβόρες διαδικασίες, που δυσχεραίνουν την καθημερινότητά του και κάνουν δύσκολη την ζωή του.

Για την αντιμετώπιση αυτών των δυσκολιών και προς την κατεύθυνση εξυγίανσης της Δημόσιας Διοίκησης, γεννήθηκαν οι ανάγκες των νέων Πληροφοριακών Συστημάτων του Μητρώου Πολιτών και της Κάρτας Πολίτη τα οποία περιγράφονται παρακάτω.

5.2. ΜΗΤΡΩΟ ΠΟΛΙΤΩΝ

Το νέο και ελπιδοφόρο πληροφοριακό σύστημα με το όνομα **«Μητρώο Πολιτών»**, είναι η μεγάλη βάση δεδομένων με τα στοιχεία των πολιτών, **η πρωτογενής πληροφορία που θα χρειαστεί για την έκδοση της «Κάρτας Πολίτη»**. Ξεκίνησε και τέθηκε σε ισχύ από τις 22 Ιανουαρίου 2018.

Το Μητρώο Πολιτών[28] είναι το μεγαλόπνοο σχέδιο του υπουργείου Εσωτερικών, με σκοπό την εθνική διασύνδεση online 1.036 υπηρεσίες Ληξιαρχείου και 325 υπηρεσίες Δημοτολογίου, καθώς και του Ειδικού Ληξιαρχείου Αθηνών. Στόχος είναι να δημιουργηθεί μία κεντρική βάση δεδομένων, που θα περιέχει όλα τα στοιχεία που αφορούν στις ληξιαρχικές πράξεις των Ελλήνων πολιτών.

Παλιότερα, οι πολίτες θα έπρεπε να προσκομίζουν σε κάθε υπηρεσία που συναλλασσόταν κάθε φορά τα ίδια πιστοποιητικά, όπως αποσπάσματα ληξιαρχείου, πιστοποιητικά οικογενειακής κατάστασης και ληξιαρχικές πράξεις γέννησης, γάμου και θανάτου. Μέσω της εφαρμογής αυτής, οι ληξιαρχικές πληροφορίες του καθενός θα παρέχονται ηλεκτρονικά στους

[28] https://www.ypes.gr/ergo-mitroo-politon-archiki

αντίστοιχους φορείς μέσω ασφαλούς διασύνδεσης των φορέων, αυτόματα και στον ελάχιστο χρόνο.

Παραδείγματος χάριν, εάν ένας δημότης Αθηναίων παντρευτεί στην Θεσσαλονίκη, το μόνο που θα χρειαστεί να κάνει είναι η δήλωση του γάμου του στο ληξιαρχείο Θεσσαλονίκης. Στη συνέχεια, η οικογενειακή του μερίδα θα ενημερωθεί αυτόματα μέσω του συστήματος, χωρίς να χρειαστεί να πάει ο ίδιος την πράξη γάμου του στο ληξιαρχείο Αθήνας.

Από τις 22 Ιανουαρίου 2018 και μετά, το Υπουργείο Παιδείας, η Ελληνική Αστυνομία, τα ΚΕΠ, το Υπουργείο Εξωτερικών, ο Ενιαίος Φορέας Κοινωνικής Ασφάλισης (ΕΦΚΑ), έχουν ολοκληρωτική πρόσβαση στα δεδομένα του Μητρώου. Επίσης, φορείς όπως η Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης (ΗΔΙΚΑ), το ΚΕΕΛΠΝΟ, η ΕΛΣΤΑΤ, το Υπουργείο Εθνικής Άμυνας και το Υπουργείο Οικονομικών, έχουν αρχίσει να έχουν πρόσβαση στα δεδομένα και διάφοροι άλλοι φορείς του δημοσίου τομέα ξεκινούν να εντάσσονται και αυτοί.

Το έργο ξεκίνησε με την εγκατάσταση κατάλληλου ηλεκτρονικού εξοπλισμού για όλες τις υπηρεσίες του ληξιαρχείου και δημοτολογίου, όπου και άρχισε η ψηφιοποίηση όλων των ληξιαρχικών δεδομένων. Η διασύνδεσή τους γινόταν σε πραγματικό χρόνο (real-time) με την κεντρική βάση δεδομένων. Τέλος, η πληροφορία που προκύπτει από την ολοκλήρωση της διαδικασίας είναι αυθεντική και δεν χρειάζεται επιπλέον σφραγίδες ή άλλα αποδεικτικά.

5.3. ΚΑΡΤΑ ΠΟΛΙΤΗ - ΝΕΑ ΤΑΥΤΟΤΗΤΑ

Όπως έχει αναφερθεί και παραπάνω, το Μητρώο Πολιτών θα αποτελέσει την πρωτογενή πληροφορία για την έκδοση της Κάρτας Πολίτη. Αντί του υπάρχοντος Δελτίου Αστυνομικής Ταυτότητας, οι πολίτες θα προμηθευτούν μία νέα ταυτότητα, σε διαστάσεις πιστωτικής κάρτας, την **Κάρτα Πολίτη - Νέα Ταυτότητα.** Για την **Κάρτα Πολίτη**, έχει δημοσιευτεί η Κοινή Υπουργική Απόφαση στην Εφημερίδα της Κυβερνήσεως με **αριθμ. 8200/0-297647/2018 (ΦΕΚ Β' 1476/27-04-2018) (Έκδοση νέου τύπου Δελτίου Ταυτότητας Ελλήνων πολιτών)**.

Η **Κάρτα Πολίτη - Νέα Ταυτότητα**[29], θα χρησιμοποιηθεί για τη φυσική ταυτοποίηση των πολιτών, αντικαθιστώντας σταδιακά την παλιά αστυνομική ταυτότητα και να εξυπηρετήσει δύο κυρίους σκοπούς:

[29] http://www.opengov.gr/ypes/?p=877

- Να αποτελέσει το κύριο μέσο της διεκπεραίωσης ηλεκτρονικών συναλλαγών με το Δημόσιο Τομέα. Ο πολίτης θα μπορεί να έχει πρόσβαση σε πλήθος ηλεκτρονικών υπηρεσιών της Δημόσιας Διοίκησης, κάνοντας την καθημερινότητα του πολύ πιο εύκολη για τον ίδιο.
- Να μπορεί να χρησιμοποιηθεί για την ψηφιακή υπογραφή εγγράφων. Ο πολίτης, μέσω διαδικτύου, θα έχει τη δυνατότητα διακίνησης εγγράφων με την ψηφιακή υπογραφή του, με στόχο την κατάργηση του χαρτιού και του ταχυδρομείου στις συναλλαγές του με το Δημόσιο.

Η Κάρτα Πολίτη έχει σχεδιαστεί με υψηλού επιπέδου χαρακτηριστικά ασφάλειας, για να εναρμονίζεται με τα διεθνώς αναγνωρισμένα πρότυπα. Κύρια μέριμνα αποτελεί η εξασφάλιση προστασίας των προσωπικών δεδομένων σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, όταν ο κάτοχος πραγματοποιεί τις ηλεκτρονικές συναλλαγές του με φορείς του Δημοσίου. Η προστασία της ιδιωτικότητας των πολιτών και της ασφάλειας των συναλλαγών αποτελούν τον κύριο σκοπό του έργου αυτού.

Νεότερες ειδήσεις αναφέρουν ότι μέσα στο 2019 θα λάβει χώρα ο τελικός διαγωνισμός των νέων ταυτοτήτων, τηρώντας την υποχρέωση εναρμόνισης με τα ευρωπαϊκά πρότυπα που έχει αναλάβει η χώρα μας. Πληροφορίες αναφέρουν ότι η μικρή καθυστέρηση που υπάρχει οφείλεται στην ενδεχόμενη αλλαγή στις αρχικές προδιαγραφές, προβλέποντας και την ύπαρξη **ψηφιακού δακτυλικού αποτυπώματος**, παράλληλα με το τσιπάκι και τα βιομετρικά στοιχεία.

5.3.1. Δομή και Τεχνικά Χαρακτηριστικά της Κάρτας Πολίτη

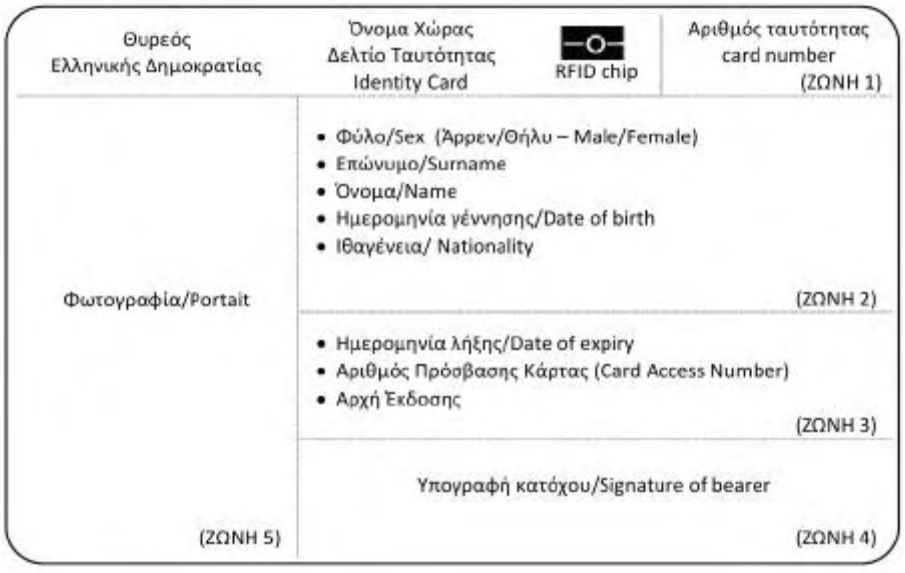
Η Κάρτα Πολίτη[30] θα έχει την μορφή και το μέγεθος μια πιστωτικής κάρτας και στην επιφάνειά της θα αναγράφονται τα στοιχεία με τα οποία πιστοποιείται ο κάτοχός της μαζί με τη φωτογραφία του**. Η καινοτομία που εισάγεται είναι το ηλεκτρονικό μικροτσίπ - chip (ελλ: πλινθίο), μέσω του οποίου θα επιτυγχάνεται η ψηφιακή αυθεντικοποίηση του πολίτη για τη χρήση των ηλεκτρονικών υπηρεσιών αλλά και η ψηφιακή υπογραφή εγγράφων.**

Οι νέες ταυτότητες έχουν δύο όψεις και χωρίζονται σε 7 «ζώνες» ασφαλείας:

[30] http://www.opengov.gr/ypes/?p=875

• Στην εμπρόσθια όψη της νέας ταυτότητας θα αναγράφονται:

1. **Ζώνη 1**: Αριθμός Ταυτότητας
2. **Ζώνη 2**:
   - **α.** Φύλο (Άρρεν/ Θήλυ),
   - **β.** Επώνυμο,
   - **γ.** Όνομα,
   - **δ.** Ημερομηνία Γέννησης,
   - **ε.** Ιθαγένεια.
3. **Ζώνη 3**:
   - **α.** Ημερομηνίας Λήξης,
   - **β.** Αριθμός Πρόσβασης Κάρτας,
   - **γ.** Αρχή Έκδοσης.
4. **Ζώνη 4**: Υπογραφή Κατόχου
5. **Ζώνη 5**: Φωτογραφία Κατόχου

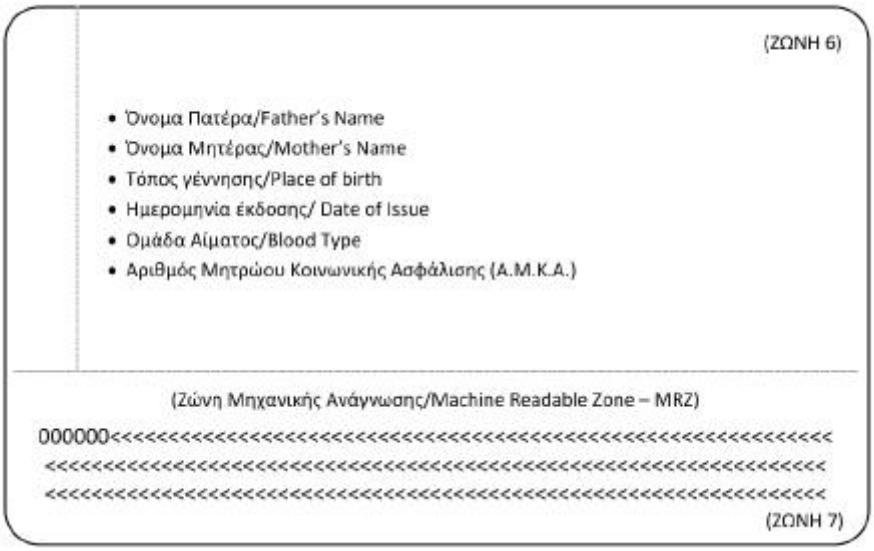


Εικόνα 96: Εμπρόσθια όψη Κάρτας Πολίτη

• Στην οπίσθια όψη της νέας ταυτότητας θα αναγράφονται:

1. **Ζώνη 6:**
    - Όνομα Πατέρα,
    - Όνομα Μητέρας,
    - Τόπος Γέννησης,
    - Ημερομηνία Έκδοσης,
    - Ομάδα Αίματος,
    - Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ),
    - Ψηφιακό δακτυλικό αποτύπωμα (Πρόκειται να ενσωματωθεί).

2. **Ζώνη 7**: Ζώνη Μηχανικής Ανάγνωσης, για αναγνώριση από ειδικά μηχανήματα σάρωσης.



Εικόνα 97: Οπίσθια όψη Κάρτας Πολίτη

Έχουν τοποθετηθεί επίσης:

1. Ο θυρεός της Ελληνικής Δημοκρατίας - Το εθνόσημο,
2. Το όνομα της χώρας - Ελληνική Δημοκρατία,
3. Ο τύπος του εγγράφου - Δελτίο Ταυτότητας,
4. Το ενσωματωμένο RFID chip.

Το ενσωματωμένο RFID chip θα περιέχει σε ψηφιακή μορφή:

1. Τη φωτογραφία του κατόχου,
2. Τα στοιχεία του κατόχου,
3. Το ύψος του κατόχου,
4. Στοιχεία που απαιτούνται για Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης, όπως ο δήμος εγγραφής, ο αριθμός δημοτολογίου και ο τόπος έκδοσης της ταυτότητας.

ΚΕΦΑΛΑΙΟ 6: ΗΛΕΚΤΡΟΝΙΚΗ ΑΝΤΑΛΛΑΓΗ ΕΓΓΡΑΦΩΝ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ

6.1. ΕΙΣΑΓΩΓΗ

Στο κεφάλαιο αυτό θα παρουσιάσουμε το πολλά υποσχόμενο έργο του Κεντρικού Συστήματος Ηλεκτρονικής Διακίνησης Εγγράφων (ΣΗΔΕ), τα πλεονεκτήματά του και τα βασικά στοιχεία της αρχιτεκτονικής του.

6.2. ΚΕΝΤΡΙΚΟ ΣΥΣΤΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΙΝΗΣΗΣ ΕΓΓΡΑΦΩΝ (ΣΗΔΕ)

Σύμφωνα με το άρθρο 3 του νόμου 3979/2011 για την ηλεκτρονική διακυβέρνηση, «**ηλεκτρονική διαχείριση εγγράφων είναι το σύνολο των ενεργειών που πραγματοποιούνται με χρήση ΤΠΕ και που αποσκοπούν στην καταχώριση, πρωτοκόλληση, οργάνωση, ταξινόμηση και συντήρηση των εγγράφων που δημιουργήθηκαν από τους φορείς του δημόσιου τομέα ή των εγγράφων που περιήλθαν σε αυτούς μέσω τρίτων».**

Προς την κατεύθυνση αυτή, στις 10 Αυγούστου του 2018, το Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης (ΨΗΠΤΕ)[31] προχώρησε στην δημοσίευση της προκήρυξης ανοιχτού διεθνούς ηλεκτρονικού διαγωνισμού, με τίτλο «**Υλοποίηση Κεντρικού Συστήματος Διακίνησης Εγγράφων, Δρομολόγησης και Διαλειτουργικότητας με Απομακρυσμένες Ψηφιακές Υπογραφές καθώς και Μηχανισμό Υποστήριξης του (helpdesk)**»[32].

Το έργο «**Κεντρικό Σύστημα Ηλεκτρονικής Ανταλλαγής Εγγράφων (ΣΗΔΕ)**» αφορά στην διακίνηση και δρομολόγηση των εγγράφων, μέσω ψηφιακών υπογραφών, μεταξύ των φορέων του δημόσιου τομέα. Μέσω των ψηφιακών τεχνολογιών, οι εργασίες θα επιταχυνθούν, θα βελτιωθούν και μακροπρόθεσμα θα αυτοματοποιηθούν. Η διακίνηση των εγγράφων θα πραγματοποιείται με διαφάνεια, αξιοπιστία και ασφάλεια και επιπλέον θα υπάρχει η

[31] http://www.mindigital.gr/

[32] http://www.mindigital.gr/attachments/article/2741/18PROC003565072.pdf

δυνατότητα να ανακτάται και να εντοπίζεται η διαδρομή τους ανά πάσα χρονική στιγμή. Όλα τα παραπάνω θα συντελέσουν στην ταχύτερη και ευκολότερη εξυπηρέτηση των πολιτών, συμβάλλοντας στην βελτίωση των υπηρεσιών που παρέχονται από τη Δημόσιο.

Στόχοι του είναι η ηλεκτρονική διασύνδεση είκοσι ένα χιλιάδων (21.000) φορέων του Δημοσίου και η παροχή εκατόν πενήντα χιλιάδων (150.000) απομακρυσμένων ψηφιακών υπογραφών σε δημοσίους υπαλλήλους. Για κάθε ψηφιακή υπογραφή που θα παρέχεται, υπολογίζεται ότι για το κράτος θα εξοικονομείται το ποσό περίπου των χιλίων ευρώ (1.000 €). Γενικότερα, για το διάστημα του ενός μόνου έτους, η εξοικονόμηση από την πλήρη λειτουργία του ΣΗΔΕ εκτιμάται στο ποσό των τριακοσίων ογδόντα 380 εκ. ευρώ.

6.2.1. Πλεονεκτήματα του ΣΗΔΕ

Τα πλεονεκτήματα που προκύπτουν από την υλοποίηση του Κεντρικού Συστήματος Ηλεκτρονικής Διαχείρισης Εγγράφων (ΣΗΔΕ) σε σχέση με το χειροκίνητο σύστημα είναι τα παρακάτω:

- Αυτοματοποίηση και βελτιστοποίηση της διεκπεραίωσης των διαδικασιών.
- Μείωση του χρόνου καθυστέρησης διακίνησης των εγγράφων.
- Εξοικονόμηση ανθρωπίνου προσωπικού και εξοικονόμηση εργατοωρών.
- Σημαντική μείωση εξόδων όπως το κόστος χαρτιού, το κόστος αναλώσιμων εκτυπωτών, το κόστος των φωτοτυπικών συσκευών, των συσκευών φαξ και των σαρωτών.
- Αύξηση της διαφάνειας και της ασφάλειας των διαδικασιών.
- Γρήγορος και εύκολος εντοπισμός των αρχειοθετημένων εγγράφων.

Όλα τα παραπάνω πλεονεκτήματα, καθιστούν επιτακτική την ανάγκη υλοποίησης και λειτουργίας του ΣΗΔΕ.

6.2.2. Αρχιτεκτονική συστήματος ΣΗΔΕ

Οι βασικές μονάδες που απαρτίζουν το έργο του ΣΗΔΕ είναι οι παρακάτω:

1. Το Σύστημα Ψηφιακών Υπογραφών (ΣΨΥ)

2. Το Σύστημα Διακίνησης Εγγράφων, Δρομολόγησης και Διαλειτουργικότητας (ΣΔΔΔ)

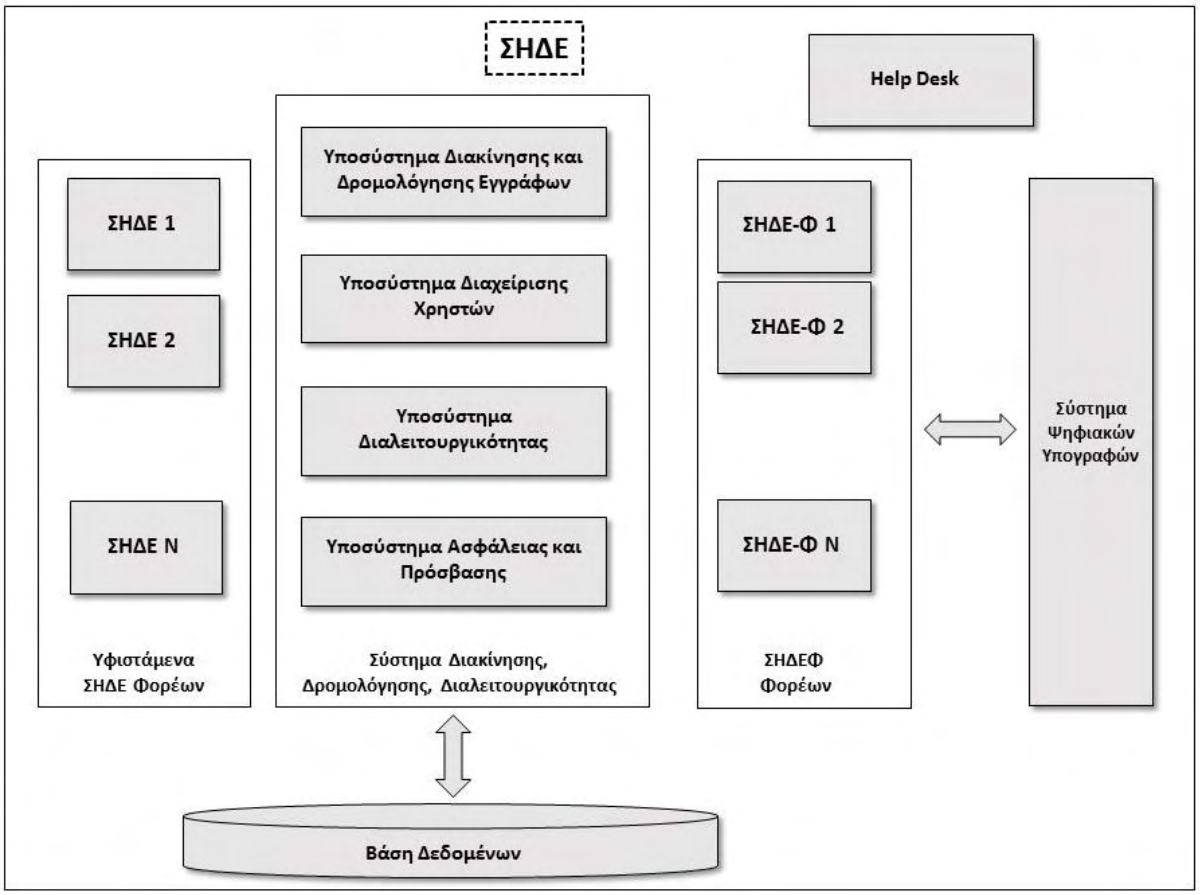
3. Τα Συστήματα Ηλεκτρονικής Διακίνησης Εγγράφων Φορέων (ΣΗΔΕ-Φ1, 2, ...,Ν)

4. Το Σύστημα Υποστήριξης Χρηστών (Help Desk)

5. Τη Βάση Δεδομένων (ΒΔ)

6. Τα σημεία διασύνδεσης με τα τοπικά ΣΗΔΕ (ΣΗΔΕ 1,2,...,N) - Οι φορείς θα έχουν την δυνατότητα να ενσωματώνουν τις εφαρμογές τους (τοπικά ΣΗΔΕ), οι οποίες θα διαλειτουργούν με το Κεντρικό ΣΗΔΕ.

Η αρχιτεκτονική του ΣΗΔΕ απεικονίζεται στο παρακάτω σχήμα:



Εικόνα 98: Αρχιτεκτονική ΣΗΔΕ

6.2.2.1. Σύστημα Απομακρυσμένων Ψηφιακών Υπογραφών (ΣΨΥ)

Το σύστημα αυτό θα προσφέρει απομακρυσμένες ψηφιακές υπογραφές μέσω μίας υποδομής ασφαλούς διάταξης έκδοσης και διαχείρισης ψηφιακών υπογραφών.

Το έργο, όπως αναφέρθηκε και παραπάνω, προβλέπει αρχικά την παροχή εκατόν πενήντα χιλιάδων (150.000) απομακρυσμένων ψηφιακών υπογραφών σε δημοσίους υπαλλήλους, μαζί

με τις απαιτούμενες άδειες χρήσης τριετούς διάρκειας. Η ΑΠΕΔ έχει οριστεί να είναι η Πρωτεύουσα Αρχή Πιστοποίησης που θα αναλάβει την έκδοση των αντίστοιχων ψηφιακών πιστοποιητικών για τις ψηφιακές υπογραφές.

6.2.2.2. Σύστημα Διακίνησης Εγγράφων, Δρομολόγησης και Διαλειτουργικότητας (ΣΔΔΔ)

Το Σύστημα Διακίνησης Εγγράφων, Δρομολόγησης και Διαλειτουργικότητας (ΣΔΔΔ) είναι το κεντρικό σύστημα για την ηλεκτρονική ανταλλαγή εγγράφων από φορέα σε φορέα.

Ειδικότερα, στο **υποσύστημα Διακίνησης και Δρομολόγησης Εγγράφων** που είναι ο κεντρικός πυλώνας του συστήματος, θα εισέρχονται όλα τα έγγραφα, όπου θα καταγράφονται και θα αποθηκεύονται. Κάθε εισερχόμενο έγγραφο θα λαμβάνει ένα μοναδικό αναγνωριστικό (unique ID) και στη συνέχεια θα προωθείται στον προορισμό του για την διεκπεραίωσή του.

Από την άλλη μεριά, ο αποστολέας του εγγράφου θα λαμβάνει ένα αποδεικτικό επιτυχούς παράδοσης της αποστολής του (proof of delivery), το οποίο θα περιλαμβάνει το μοναδικό αναγνωριστικό (unique ID) και ένα μοναδικό αλφαριθμητικό, που του επιτρέπει να παρακολουθεί την κατάσταση του εγγράφου του. Τέλος, το έγγραφο θα προωθείται στον τελικό παραλήπτη του.

6.2.2.3.Συστήματα Ηλεκτρονικής Διακίνησης Εγγράφων Φορέων (ΣΗΔΕ-Φ)

Για τους φορείς που δεν έχουν τοπικά ΣΗΔΕ και χρειάζεται να υλοποιούν μόνο απλές ροές εργασίας, θα δημιουργηθεί το Σύστημα Ηλεκτρονικής Διακίνησης Εγγράφων Φορέων (ΣΗΔΕ-Φ). Η απλή ροή εργασίας ή ροή εργασίας ενός βήματος, είναι π.χ. όταν διαμέσου του κεντρικού ΣΗΔΕ ένας φορέας δημιουργεί το ηλεκτρονικό του πρωτόκολλο και έπειτα προχωρά στην χρέωση των εισερχομένων έγγραφών του στους δικούς του υπαλλήλους - χρήστες.

Συνεπώς, οι φορείς αυτοί θα έχουν την δυνατότητα μέσω του ΣΗΔΕ-Φ, να υλοποιούν υπηρεσίες ηλεκτρονικού πρωτοκόλλου, διαχείρισης εγγράφων και ψηφιακής υπογραφής μέσω αυτοματοποιημένης ροή εργασίας ενός βήματος (one-step workflow). Η παραπάνω διαδικασία

θα γίνεται μέσω νεφοϋπολογιστικής (cloud computing)[33] υποδομής που είναι η κοινή χρήση απομακρυσμένων από τον τελικό χρήστη υπολογιστικών συστημάτων μέσω διαδικτύου.

6.2.2.4. Εργαλείο Υποστήριξης Χρηστών (Help Desk Software Tool)

Το εργαλείο υποστήριξης χρηστών (Help Desk Software Tool) έχει σκοπό την υποστήριξη των χρηστών του συστήματος όσον αφορά τη λειτουργικότητα των συστημάτων, όπως του κεντρικού συστήματος ΣΗΔΕ, των ΣΗΔΕ-Φ, των ψηφιακών υπογραφών κ.α.

Θα δημιουργηθεί ένα γραφείο αρωγής χρηστών, το οποίο θα στελεχωθεί από άρτια καταρτισμένους υπαλλήλους και το οποίο θα έχει αρμοδιότητα την επίλυση των όποιων προβλημάτων και απορίων των χρηστών.

Το εργαλείο θα πρέπει να έχει σχεδιαστεί σε φιλικό προς το χρήστη περιβάλλον (user friendly GUI) και να είναι εύχρηστο. Η επικοινωνία των χρηστών και η υποστήριξή τους θα γίνεται ηλεκτρονικά και σε απευθείας σύνδεση (online).

6.2.2.5. Βάση δεδομένων

Η βάση δεδομένων είναι το μέρος όπου αποθηκεύονται τα δεδομένα όλων των συστημάτων και θα πρέπει να πληροί τις παρακάτω προδιαγραφές:

- Ασφάλεια
- Υψηλή απόδοση
- Τμηματοποίηση (partitioning) των δεδομένων
- Δυνατότητα συμπίεσης (compression) δεδομένων για εξοικονόμηση χωρητικότητας
- Δυνατότητα εξόρυξης δεδομένων (data mining)
- Δυνατότητα κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων

6.2.2.6. Σημεία διασύνδεσης με τα τοπικά ΣΗΔΕ (ΣΗΔΕ 1,2,...,N)

Για τους φορείς που έχουν ανάγκη υλοποίησης σύνθετων ροών εργασίας, και έχουν ήδη εγκαταστήσει τοπικά ΣΗΔΕ θα μπορέσουν να ενσωματώσουν τις εφαρμογές αυτές ώστε να

[33] https://en.wikipedia.org/wiki/Cloud_computing

διαλειτουργούν με το Κεντρικό ΣΗΔΕ. Αυτό θα επιτευχθεί αρχικά μέσω της διασύνδεση των τοπικών συστημάτων ΣΗΔΕ μεταξύ τους, και στη συνέχεια μέσω της διασύνδεσης τους με το Κεντρικό ΣΗΔΕ, ακολουθώντας συγκεκριμένες προδιαγραφές και πρωτοκόλλα επικοινωνίας.

ΚΕΦΑΛΑΙΟ 7: ΣΥΜΠΕΡΑΣΜΑΤΑ

Αναλύοντας τα παραπάνω κεφάλαια και παρατηρώντας την κατάσταση στην Ελλάδα τα τελευταία χρόνια, συμπεραίνουμε ότι έχουν γίνει αλματώδεις προσπάθειες για τον εκσυγχρονισμό της Δημόσιας Διοίκησης. Ο Δημόσιος Τομέας χαρακτηριζόταν ανέκαθεν ως η *«Αχίλλειος πτέρνα»* για την Ελληνική κοινωνία και αποτελούσε ένα σημείο αμφισβήτησης της διαφάνειας των συναλλαγών των πολιτών εδώ και πολλά χρόνια. Χρέος των δημόσιων δομών είναι η επικοινωνία και η συνεργασία μεταξύ τους ώστε να είναι σε θέση να προσφέρουν ποιοτικές υπηρεσίες προς τους πολίτες. Η πιο ενδεδειγμένη μέθοδος ως προς την καλύτερη λειτουργία τους είναι η ψηφιακή υπογραφή και η ηλεκτρονική ανταλλαγή και διακίνηση των εγγράφων.

Μέσω της χρήσης της ψηφιακής υπογραφής εξασφαλίζεται η ασφαλής επικοινωνία μεταξύ χρηστών οι οποίοι αποδεικνύουν την ταυτότητα τους, και επιτυγχάνουν την ασφαλή μεταφορά των ηλεκτρονικών μηνυμάτων, χωρίς να υπάρχει κίνδυνος υποκλοπής και αλλοίωσής τους. Επίσης, εξασφαλίζεται σημαντικά η μείωση κόστους σε εκτυπώσεις, επικυρώσεις, έξοδα αποστολής και καταργείται η ανάγκη για «φυσική» αρχειοθέτηση (προστασία περιβάλλοντος). Επιπρόσθετα, επιτυγχάνεται εξοικονόμηση χρόνου εργασίας, περιορίζοντας σημαντικά την γραφειοκρατία.

Μέσω της ηλεκτρονικής διακίνησης των εγγράφων, η οποία θα αφορά όλα τα υπουργεία και τους λοιπούς φορείς του Δημοσίου, θα δημιουργηθεί μια κεντρική υποδομή ανταλλαγής εγγράφων μεταξύ του συνόλου των φορέων χρησιμοποιώντας την τεχνολογία των προηγμένων ψηφιακών υπογραφών. Η καινοτομία που εισάγεται είναι ο ορισμός της διαδρομής των εγγράφων από τον φορέα, ενισχύοντάς την δυνατότητα ανάκτησης και εντοπισμού του «ίχνους» τους ανά πάσα χρονική στιγμή. Συνεπώς, η διακίνηση των εγγράφων θα πραγματοποιείται με αξιοπιστία, ασφάλεια και απόλυτη διαφάνεια.

Σύμφωνα με τις πιο πρόσφατες εξελίξεις, υπεγράφη τον Μάιο του 2019 η σύμβαση υλοποίησης του έργου «Κεντρικό Σύστημα Ηλεκτρονικής Διακίνησης Εγγράφων (ΣΗΔΕ)» για την ένταξη όλων των φορέων του Δημοσίου στο Σύστημα Ηλεκτρονικής Διακίνησης Εγγράφων. Το χρονοδιάγραμμα του έργου προβλέπει την ολοκλήρωσή του σε διάστημα δέκα (10) μηνών και ακολούθως έχει προβλεφθεί ένα διάστημα δύο (2) μηνών όπου θα τεθεί το έργο σε απαραίτητη δοκιμαστική λειτουργία .

Συμπερασματικά, σε ένα χρόνο από τώρα και στα μέσα του 2020, θα είμαστε σε θέση να κάνουμε λόγο για την άμεση υλοποίηση και εφαρμογή του μεγαλόπνοου αυτού σχεδίου. Οι πολίτες θα είναι αρωγοί και κοινωνοί ενός καλύτερου Δημοσίου Τομέα, με διαφάνεια και ταχύτητα στη διεκπεραίωση αιτημάτων, με καλύτερη συνεργασία υπηρεσιών και εύρυθμη λειτουργία φορέων, συμβάλλοντας έτσι στην κατάργηση του ως τώρα «πελατειακού κράτους» και στην σταδιακή βελτίωση της καθημερινότητάς τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΝΑΦΟΡΕΣ

An Overview of Cryptography. (2019, Απρίλιος 10). Ανάκτηση από http://www.garykessler.net/library/crypto.html#skc

E-government. (2019, Μάρτιος 15). Ανάκτηση από en.wikipedia.org/wiki/E-government

Information Technology. (2019, Μάρτιος 20). Ανάκτηση από https://en.wikipedia.org/wiki/Information_technology

Kerberos: The Network Authentication Protocol. (2019, Απρίλιος 10). Ανάκτηση από http://web.mit.edu/Kerberos

PGP - Pretty Good Privacy. (2019, Απρίλιος 10). Ανάκτηση από https://en.wikipedia.org/wiki/Pretty_Good_Privacy

RSA κρυπταλγόριθμος . (2019, Μάρτιος 20). Ανάκτηση από https://el.wikipedia.org/wiki/RSA

USB token. (2019, Απρίλιος 10). Ανάκτηση από https://el.wikipedia.org/wiki/USB_Token

Ακαδημαϊκό Διαδίκτυο (GUnet) . (2019, Απρίλιος 20). Ανάκτηση από https://www.gunet.gr

Ανοικτή Διακυβέρνηση. (2019, Μάρτιος 15). Ανάκτηση από http://www.opengov.gr

Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ). (2019, Απρίλιος 10). Ανάκτηση από http://www.aped.gov.gr/

Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων. (2019, Μάϊος 2). Ανάκτηση από https://www.eett.gr

Εθνική Πύλη ΕΡΜΗΣ. (2019, Απρίλιος 15). Ανάκτηση από http://www.ermis.gov.gr

Έξυπνη Κάρτα. (2019, Μάρτιος 10). Ανάκτηση από https://en.wikipedia.org/wiki/Smart_card

Ηλεκτρονική Διακυβέρνηση. (2019, Μάρτιος 20). Ανάκτηση από http://www.minadmin.gov.gr/?page_id=12126

Ηλεκτρονική Υποβολή Αιτήματος Έκδοσης Ψηφιακών Πιστοποιητικών Ermis. (2019, Μάρτιος 10). Ανάκτηση από http://www.aped.gov.gr/images/steps1-6/step_2_submit_application_for_pki_certificates_v2_2.pdf

Κανονισμός (ΕΕ) αριθ. 910/2014. (2014, Ιούλιος 23). *Σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ.* Ευρωπαϊκό Κοινοβούλιο.

Κάρτα Πολίτη. (2019, Απρίλιος 10). Ανάκτηση από http://www.opengov.gr/ypes/?p=877

Κέντρο Ηλεκτρονικής Διακυβέρνησης ΑΠΘ. (2019, Απρίλιος 15). Ανάκτηση από https://it.auth.gr/el

Κοινωνία της Πληροφορίας. (2019, Μάρτιος 10). Ανάκτηση από http://www.ktpae.gr/

Κρυπτογράφηση. (2019, Ιανουάριος 15). Ανάκτηση από https://en.wikipedia.org/wiki/Cryptography

Μητρώο Πολιτών. (2019, Απρίλιος 15). Ανάκτηση από https://www.ypes.gr/ergo-mitroo-politon-archiki

Νόμος 3979/2001. (16/06/2001). *Για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις.*

Π.Δ. 150/2001. (25.06.2001). *Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.*

Πιστοποιητικό Δημόσιου Κλειδιού. (2019, Απρίλιος 10). Ανάκτηση από https://en.wikipedia.org/wiki/Public_key_certificate

Προκήρυξη Διεθνούς Ανοιχτού Ηλεκτρονικού Διαγωνισμού με τίτλο: «Υλοποίηση Κεντρικού Συστήματος Διακίνησης Εγγράφων, Δρομολόγησης και Διαλειτουργικότητας με απομακρυσμένες ψηφιακές υπογραφές καθώς και Μηχανισμό Υποστήριξής του (helpdesk)». (2019, Μάρτιος 10). Ανάκτηση από http://www.mindigital.gr/attachments/article/2741/18PROC003565072.pdf

Ρύθμιση συσκευής για χρήση της Ακαδημαϊκής ταυτότητας. (2019, Μάρτιος 15). Ανάκτηση από https://it.auth.gr/el/setupAcademicId

Στρατηγική για την Ηλεκτρονική Διακυβέρνηση 2014-2020. (2019, Μάρτιος 15). Ανάκτηση από http://www.minadmin.gov.gr/wp-content/uploads/20140415_egov_strategy.pdf

Συνάρτηση Κατατεμαχισμού. (2019, Μάρτιος 15). Ανάκτηση από https://en.wikipedia.org/wiki/Hash_function

Τεχνικά Χαρακτηριστικά της Κάρτας Πολίτη. (2019, Απρίλιος 10). Ανάκτηση από http://www.opengov.gr/ypes/?p=875

Υπηρεσία Ανάπτυξης Πληροφορικής. (2019, Απρίλιος 20). Ανάκτηση από http://yap.gov.gr/

Υπογραφή σύμβασης υλοποίησης της ηλεκτρονικής διακίνησης εγγράφων στο Δημόσιο. (n.d.). Ανάκτηση από https://www.naftemporiki.gr/story/1474137/ypegrafi-i-sumbasi-ulopoiisis-tis-ilektronikis-diakinisis-eggrafon

Υποδομή Δημοσίου Κλειδιού HARICA. (2019, Ιανουάριος 20). Ανάκτηση από https://app.harica.gr

Υποδομή Δημοσίου Κλειδιού ΑΠΘ. (2019, Απρίλιος 10). Ανάκτηση από https://pki.auth.gr/

Υπολογιστικό Νέφος. (2019, Μάρτιος 10). Ανάκτηση από https://en.wikipedia.org/wiki/Cloud_computing

Υπουργείο Διοικητικής Ανασυγκρότησης. (2019, Μάρτιος 10). Ανάκτηση από http://www.minadmin.gov.gr/

Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης. (2019, Μάρτιος 10). Ανάκτηση από http://www.mindigital.gr/

Φ.Ε.Κ. 1317/Β'/23.04.2012. (2012). *Ρυθμίσεις για το Ηλεκτρονικό Δημόσιο Έγγραφο.*

ΦΕΚ Β' 1476/27.04.2018. (2018). *Έκδοση νέου τύπου Δελτίου Ταυτότητας Ελλήνων πολιτών.*

Ψηφιακή Υπογραφή. (2019, Μάρτιος 10). Ανάκτηση από https://en.wikipedia.org/wiki/Digital_signature