



Πανεπιστήμιο Αιγαίου

**Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών
Συστημάτων**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΡΒΑΝΙΤΗ ΚΟΚΩΝΗ ΑΜ 321/2013016

**ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΜΕ ΒΑΣΗ ΤΟ ΕΛΛΗΝΙΚΟ ΚΑΙ ΕΥΡΩΠΑΪΚΟ
ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ - Ο ΒΑΘΜΟΣ ΑΝΑΠΤΥΞΗΣ ΤΩΝ ΨΗΦΙΑΚΩΝ
ΥΠΟΓΡΑΦΩΝ ΣΤΟΝ ΔΗΜΟΣΙΟ ΚΑΙ ΙΔΙΩΤΙΚΟ ΤΟΜΕΑ**

Επιβλέπουσα καθηγήτρια: Ευαγγελία Μήτρου

Σάμος, Ιανουάριος, 2021



Ευχαριστίες

Στους γονείς μου **Παναγιώτη** και **Ειρήνη** αλλά και στα αδέρφια μου **Χριστόδουλο**, **Ζωή** και **Ανέστη** για τη συνεχή στήριξη, κατανόηση και εμπιστοσύνη καθ' όλη τη διάρκεια των σπουδών μου,

στις καλές μου φίλες **Ελένη**, **Αλεξία** και **Νικολέτα** για την αμέριστη υποστήριξη και το αμείωτο ενδιαφέρον τους όλα αυτά τα χρόνια των σπουδών μου,

στην καλή φίλη, συμφοιτήτρια και συνάδελφο **Αλεξάνδρα** για την ανοχή, την ενθάρρυνση αλλά και την πολύ καλή συνεργασία μας,

στην κα **Λίλιαν Μήτρου**, επιβλέπουσα καθηγήτρια της διπλωματικής μου εργασίας, για την επιστημονική καθοδήγηση, εμπιστοσύνη και επιμονή που μου έδειξε όλο αυτό το διάστημα από την αρχή μέχρι και την ολοκλήρωση της εργασίας.



Περίληψη

Η παρούσα μελέτη αφορά τα συστήματα ηλεκτρονική διακυβέρνησης και την ηλεκτρονική υπογραφή στον δημόσιο και ιδιωτικό τομέα της Ελλάδας, καθώς και το νομικό πλαίσιο στο οποίο εντάσσονται στην εκάστοτε περίπτωση.

Αναλυτικότερα, στο πρώτο κεφάλαιο, γίνεται αναφορά στις εισαγωγικές έννοιες που σχετίζονται με τα ηλεκτρονικά μέσα και την ηλεκτρονική υπογραφή. Ακόμη, σχολιάζεται ο τρόπος που εφαρμόζεται η γνησιότητα της ηλεκτρονικής υπογραφής, αλλά και το σύγχρονο νομικό πλαίσιο. Επιπλέον, υπογραμμίζονται τα εγκεκριμένα πιστοποιητικά, και η εφαρμογή των νεωτεριστικών νόμων της Ελλάδας για τις ηλεκτρονικές συμβάσεις και τις συμβάσεις στο διαδίκτυο.

Στο δεύτερο κεφάλαιο, δίνεται έμφαση στις ηλεκτρονικές υπογραφές και πώς εφαρμόζονται στο δημόσιο τομέα. Για την ανάλυση του παρόντος κεφαλαίου σχολιάζονται τα συστήματα ηλεκτρονικής διαχείρισης του δημόσιου τομέα.

Στο τρίτο κεφάλαιο, σχολιάζεται η εφαρμογή της ηλεκτρονικής υπογραφής στον ιδιωτικό τομέα. Πιο συγκεκριμένα, γίνεται αναφορά στην ηλεκτρονική τιμολόγηση, το νομικό πλαίσιο που υπόκειται, οι απαιτήσεις ασφαλείας που υπάρχουν, οι τρέχουσες τάσεις της αγοράς και τα διάφορα επιχειρησιακά μοντέλα ηλεκτρονικής τιμολόγησης. Τέλος, καταγράφονται τα συνολικά πορίσματα της μελέτης.

Λέξεις-Κλειδιά: ηλεκτρονική υπογραφή, δημόσιος τομέας, ιδιωτικός τομέας, ηλεκτρονική διακυβέρνηση, νομικό πλαίσιο



Abstract

The present study concerns the e-government systems and the e-signature in the public and private sector of Greece, as well as the legal framework in which they are included in each case.

More specifically, in the first chapter, reference is made to the introductory concepts related to electronic media and electronic signature. It also comments on the way in which the authenticity of the electronic signature is applied, as well as the modern legal framework. In addition, the approved certificates and the application of the modernist laws of Greece for electronic contracts and contracts on the internet are underlined.

The second chapter focuses on electronic signatures and how they are implemented in the public sector. For the analysis of this chapter, the electronic management systems of the public sector are commented.

In the third chapter, the application of electronic signature in the private sector is commented. More specifically, reference is made to e-invoicing, the legal framework it is subject to, security requirements that exist, current market trends and the various business models of e-invoicing. Finally, the overall findings of the study are recorded.

Keywords: e-signature, public sector, private sector, e-government, legal framework



Πίνακας περιεχομένων

Περίληψη	3
Abstract	4
Εισαγωγή.....	7
ΚΕΦΑΛΑΙΟ 1ο Ηλεκτρονικά μέσα και ηλεκτρονικές υπογραφές	9
Ηλεκτρονικά έγγραφα.....	9
Διάκριση ηλεκτρονικών εγγράφων	9
Παράδειγμα υποστολής και λήψης ηλεκτρονικού εγγράφου με την χρήση του Outlook.....	10
Ηλεκτρονικές υπογραφές.....	12
Η έννοια της ηλεκτρονικής υπογραφής	13
Η πιστοποίηση του ΠΥΠ για την έκδοση πιστοποιητικών γνησιότητας	18
Νομικά πλαίσια Ηλεκτρονικών εγγράφων και Ψηφιακών υπογραφών.....	19
Ο κανονισμός 910/2014 για τις ηλεκτρονικές υπογραφές	19
Εγκεκριμένες ηλεκτρονικές υπογραφές	22
Εγκεκριμένα πιστοποιητικά	22
Υπηρεσίες εμπιστοσύνης	24
Ευθύνη εγκεκριμένων παρόχων	25
Η εφαρμογή του Κανονισμού 910/2014 στην Ελλάδα	28
Ηλεκτρονικές συμβάσεις	31
Συμβάσεις στο διαδίκτυο	33
ΚΕΦΑΛΑΙΟ 2ο Η τεχνολογία στο δημόσιο τομέα και ψηφιακή κυβέρνηση.....	37
Ηλεκτρονική διακυβέρνηση και ηλεκτρονικές συμβάσεις στον δημόσιο τομέα	38
Το εθνικό δίκτυο δημοσίας διοίκησης ΣΥΖΕΥΞΙΣ.....	40
Η Διαδικτυακή Πύλη ermis.gov.gr και οι υπηρεσίες της στους πολίτες.....	41
Οι διαδικτυακές πύλες (portals) της κυβέρνησης	41



Υπηρεσίες της Κυβερνητικής Διαδικτυακής Πύλης ΕΡΜΗΣ.....	42
Άνοιγμα Ηλεκτρονικής Θυρίδας.....	44
Αρχή πιστοποίησης του ελληνικού δημοσίου.....	45
Οφέλη.....	49
Νόμος 4727/2020	51
ΚΕΦΑΛΑΙΟ 3 ^ο Εφαρμογές ηλεκτρονικών υπογράφων στον ιδιωτικό τομέα	57
Ηλεκτρονική τιμολόγηση (e-Invoicing)	57
Νομικό πλαίσιο	60
Απαιτήσεις ασφαλείας.....	61
Συμπεράσματα	63
Βιβλιογραφία	64



Εισαγωγή

Η κοινωνία της πληροφορίας είναι μια κοινωνία στην οποία η παραγωγή, διανομή, χρήση, ολοκλήρωση και διαχείριση πληροφοριών είναι σημαντικές οικονομικές, πολιτικές και πολιτιστικές δραστηριότητες. (Ιγγλεζάκης, 2012)

Με την εφαρμογή της πληροφορικής σε διάφορες οικονομικές δραστηριότητες, ο όρος κοινωνία της πληροφορίας έχει εισαχθεί. Ο στόχος της κοινωνίας της πληροφορίας είναι να αποκτήσει ένα ανταγωνιστικό πλεονέκτημα διεθνώς μέσω της χρήσης της τεχνολογίας πληροφοριών με δημιουργικό και παραγωγικό τρόπο. Η κοινωνία της πληροφορίας θεωρείται ο διάδοχος της βιομηχανικής κοινωνίας. (Ιγγλεζάκης, 2012)

Οι πολίτες που είναι σε θέση να συμμετάσχουν σε αυτήν τη μορφή κοινωνίας συχνά ονομάζονται "ψηφιακοί πολίτες". Αυτό είναι ένα από τα πολλά «ονόματα» που δείχνουν ότι οι σύγχρονοι άνθρωποι εισέρχονται σε μια νέα κοινωνική φόρμα. (Ιγγλεζάκης, 2012)

Ως εκ τούτου, η «κοινωνία της πληροφορίας» θεωρείται μια συλλογή σημαντικών σχέσεων που εμφανίζονται και εξαρτώνται από την τεχνολογία των πληροφοριών. Ο όρος αρχικά περιελήφθη στο κοινοτικό δίκαιο. (Ιγγλεζάκης, 2012)

Η τεχνολογία των πληροφοριών, ιδίως το Διαδίκτυο και τα κινητά τηλέφωνα, έχουν συμβάλει στην ανάπτυξη της κοινωνίας της πληροφορίας. Αυτός ο τομέας αντιπροσωπεύει περίπου το 4% της απασχόλησης στην Ευρωπαϊκή Ένωση (ΕΕ). Η ΕΕ επιδιώκει να προωθήσει την ανάπτυξη και τη διάδοση νέων τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) σύμφωνα με τα άρθρα 179 έως 190 της επιχειρησιακής συνθήκης ΕΕ (ΣΛΕΕ). (Ιγγλεζάκης, 2008)

Η Ευρωπαϊκή Ένωση ολοκλήρωσε την απελευθέρωση της ευρωπαϊκής αγοράς τηλεπικοινωνιών το 1998. Ειδικότερα, το άρθρο 12 της οδηγίας 98/34 / ΕΚ (22-6-1998) (αναθεωρημένο από την οδηγία 98/48 / ΕΚ) ορίζει την έννοια της εξυπηρέτησης της κοινωνίας της πληροφορίας. (Ιγγλεζάκης, 2008)

Έκτοτε, το πλαίσιο αναθεωρήθηκε δύο φορές το 2003 και το 2009. Το τελευταίο πακέτο τηλεπικοινωνιών (2009) στοχεύει στη διασφάλιση θεμιτού ανταγωνισμού μεταξύ φορέων τηλεπικοινωνιών. (Ιγγλεζάκης, 2012)



Η έννοια της "υπηρεσίας κοινωνίας της πληροφορίας" αναφέρεται σε οποιαδήποτε υπηρεσία που παρέχεται εξ αποστάσεως έναντι αμοιβής από τους χειριστές της κατόπιν προσωπικού αιτήματος του παραλήπτη, με τη βοήθεια ηλεκτρονικού εξοπλισμού. (Ιγγλεζάκης, 2012)



ΚΕΦΑΛΑΙΟ 1ο Ηλεκτρονικά μέσα και ηλεκτρονικές υπογραφές

Ηλεκτρονικά έγγραφα

Ένα ηλεκτρονικό έγγραφο θεωρείται ένα σύνολο δεδομένων που έχουν εγγραφεί σε υπολογιστή, τα οποία μπορούν να εκτυπωθούν να εμφανιστούν στην οθόνη με ανταγωνιστικό τρόπο μετά από την επεξεργασία. Δηλαδή, το πρωτότυπο ηλεκτρονικό έγγραφο είναι καταχωρημένο στη επιφάνεια του σκληρού δίσκου του υπολογιστή. Η νομολογία είναι σύμφωνη με αυτόν τον ορισμό. Τα ηλεκτρονικά αρχεία ανήκουν στη μηχανική απεικόνιση που αναφέρεται στο άρθρο 444, παράγραφος 1γ του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα, και είναι αδιαμφισβήτητα. Οι ηλεκτρονικές υπογραφές είναι ο πιο σημαντικός παράγοντας για την επαλήθευση της γνησιότητας των ηλεκτρονικών εγγράφων. Τα ηλεκτρονικά έγγραφα θεωρούνται υποστάσεις με ηλεκτρονική και με φυσική υπόσταση. Προφανώς, η διαφορά μεταξύ ενός ηλεκτρονικού εγγράφου και ενός παραδοσιακού εγγράφου έγκειται κυρίως στη πραγματοποίηση της υπογραφής του, όπου η αυθεντικότητα του εγγράφου καθορίζεται και ορίζεται στο άρθρο 444, παράγραφος 2, του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα. Το ηλεκτρονικό έγγραφο είναι το σημαντικότερο μέσο για τη διεξαγωγή του ηλεκτρονικού εμπορίου. (Δελούκα-Ιγγλέση, 2015)

Διάκριση ηλεκτρονικών εγγράφων

Με βάση αυτόν τον ορισμό, χωρίζουμε τα ηλεκτρονικά έγγραφα σε:

- 1) Το πρωτότυπο ηλεκτρονικό έγγραφο με ηλεκτρονικό υλικό, το ηλεκτρονικό έγγραφο καταχωρείται σε ηλεκτρονική μορφή σε μαγνητικά υλικά όπως σκληρός δίσκος, δισκέτα και το κείμενο που καθορίζεται από τον εκδότη του είναι καταχωρημένο.
- 2) Αντιγραφή σύμφωνα με το πρωτότυπο. Με αυτό τον τρόπο, για παράδειγμα, ένα φαξ είναι ένα αντίγραφο που φτάνει στη συσκευή λήψης. Με άλλα λόγια, είναι είτε επανεκτύπωση του πρωτότυπου εγγράφου που φθάνει στο τερματικό, είτε το πρωτότυπο κείμενο στο ηλεκτρονικό χαρτί εγγράφου το οποίο θα φαίνεται στη μνήμη του υπολογιστή.

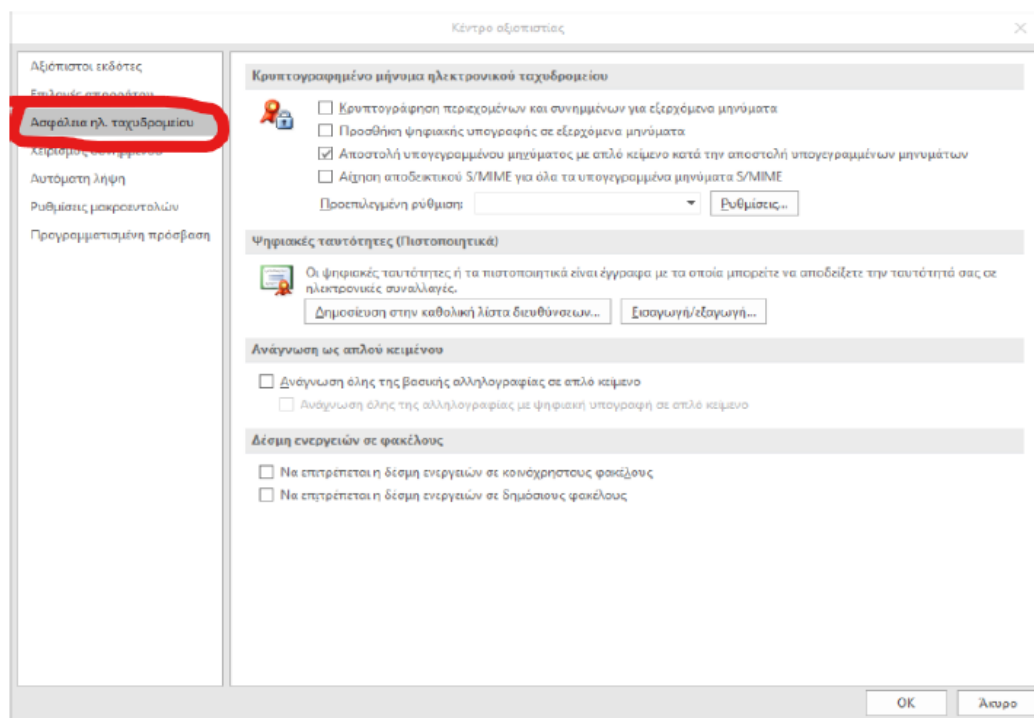
(Μανιώτης, 1998)



Παράδειγμα υποστολής και λήψης ηλεκτρονικού εγγράφου με την χρήση του Outlook

Η ψηφιακή υπογραφή μας προσδιορίζει / επιβεβαιώνει ως υπογράφων έγγραφο και επιτρέπει στον παραλήπτη του εγγράφου να επιβεβαιώσει ότι κανείς δεν έχει τροποποιήσει το περιεχόμενο του εγγράφου από τότε που υπογράφηκε το έγγραφο. Η υπογραφή, η κρυπτογράφηση και η αναγνωσιμότητα θα διαφέρουν ανάλογα με την εφαρμογή. Σε αυτό το παράδειγμα, θα χρησιμοποιήσουμε το Microsoft Outlook για την αποστολή και λήψη υπογεγραμμένων εγγράφων.

Πρώτον, είναι απαραίτητο να ρυθμιστεί το πρόγραμμα ώστε να περιλαμβάνει την υπογραφή μας. Για να το κάνετε αυτό, μεταβείτε στο Αρχείο-> Επιλογές-> Κέντρο αξιοπιστίας-> Ασφάλεια email. Το μενού θα πρέπει να μοιάζει με την ακόλουθη εικόνα:

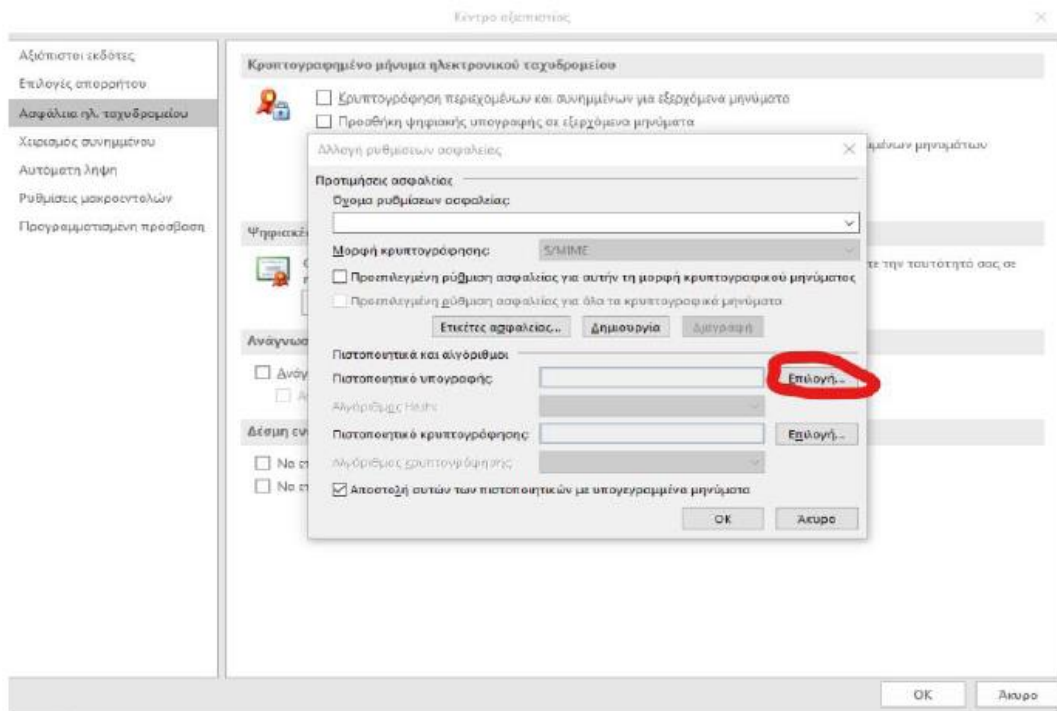


Στην καρτέλα αυτή της εικόνας επιλέγονται οι ρυθμίσεις και θα εμφανιστεί η καρτέλα:



Διπλωματική Εργασία

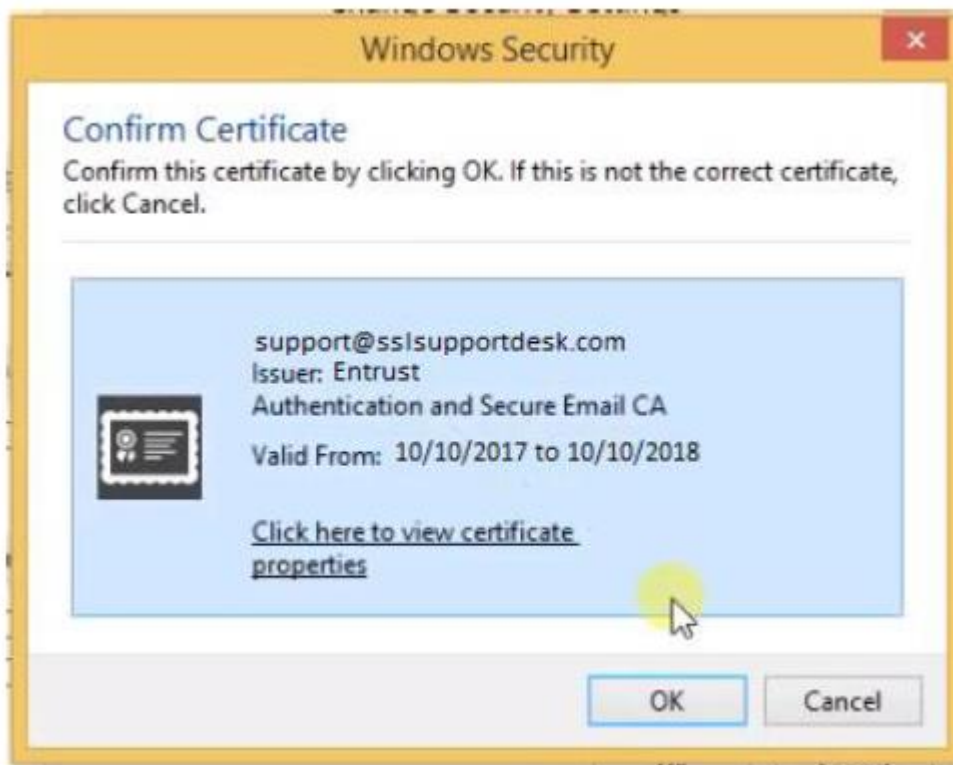
Τίτλος Μελέτης: Ψηφιακή Υπογραφή με βάση το Ελληνικό και Ευρωπαϊκό Νομοθετικό Πλαίσιο – Ο Βαθμός Ανάπτυξης των Ψηφιακών Υπογραφών στον Δημόσιο και Ιδιωτικό Τομέα
Κοκώνη Αρβανίτη



Στην συνέχεια, στην επιλογή πιστοποιητικό υπογραφής -> και μετά τοποθετούμε την ψηφιακή υπογραφή που αποκτήσαμε από εγκεκριμένο πάροχο. Δεδομένου ότι η διαδικασία έγκρισης και απόκτησης ενός τέτοιου πιστοποιητικού είναι πολύ μεγάλη, για εξοικονόμηση χώρου, θα δείξουμε μόνο ένα παράδειγμα παραλείποντας τη



διαδικασία. Βλέπουμε την εμφάνιση του πιστοποιητικού στην παρακάτω εικόνα:



Αφού επιλεγθεί το OK, είναι έτοιμο για αποστολή ένα υπογεγραμμένο ηλεκτρονικό έγγραφο. Κάντε κλικ στο Νέο μήνυμα και δημιουργήστε ένα μήνυμα. Τώρα όλα τα εξερχόμενα μηνύματα θα υπογράφονται ψηφιακά.

Ηλεκτρονικές υπογραφές

Τα ακόλουθα θα εξετάσουν και θα αναλύσουν την ηλεκτρονική υπογραφή και τον διαχωρισμό της. Θα αναφερθούν οι τύποι ηλεκτρονικών υπογραφών και ειδικών κατηγοριών ψηφιακών υπογραφών. Επειδή οι ψηφιακές υπογραφές εφαρμόζονται χρησιμοποιώντας τεχνολογία κρυπτογράφησης, οι βασικές μέθοδοι κρυπτογράφησης θα επανεξεταστούν, εστιάζοντας στην τεχνολογία κρυπτογράφησης που χρησιμοποιείται για την ανταλλαγή μηνυμάτων διαφόρων συναλλαγών.

Σύμφωνα με το νόμο 4761/2020 «*Ηλεκτρονική υπογραφή αποτελούν τα δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή και τα οποία χρησιμοποιούνται από τον υπογράφο για να υπογράψει.*»



Η έννοια της ηλεκτρονικής υπογραφής

Η κρυπτογραφία είναι μια επιστήμη που έχει σχεδιαστεί για την προστασία των δεδομένων και παρέχει εργαλεία και μεθόδους για τη μετατροπή των δεδομένων σε μη αναγνώσιμες μορφές. Ο σκοπός αυτής της επιστήμης είναι να αποτρέψει την πρόσβαση μη εξουσιοδοτημένων χρηστών στα δεδομένα, διατηρώντας έτσι το περιεχόμενο των δεδομένων εμπιστευτικό. Στην τρέχουσα κατάσταση της τεχνολογίας στις περισσότερες κοινωνίες, ο καθένας μπορεί εύκολα να αποκτήσει πρόσβαση σε έναν υπολογιστή ή ψηφιακή συσκευή που μπορεί να συνδεθεί στο δίκτυο. Με βάση τα παραπάνω, οι χρήστες μπορούν πλέον να πραγματοποιούν ηλεκτρονικές συναλλαγές. Αυτό δημιουργεί πολλά νέα προβλήματα, ένα από τα οποία είναι η ανάγκη εύρεσης ενός εγγράφου ισοδύναμου με μια χειρόγραφη υπογραφή για την επαλήθευση της αυθεντικότητας του εγγράφου. Αυτό το πρόβλημα λύνει αυτό που ονομάζουμε ηλεκτρονικές υπογραφές. (Bose & Vijayakumar, 2016)

Αν και υπάρχει συχνά σύγχυση μεταξύ των εννοιών της ηλεκτρονικής υπογραφής και της ψηφιακής υπογραφής, πρέπει να σημειωθεί ότι αυτές είναι διαφορετικές έννοιες. Ειδικότερα, όπως ήδη επισημάνθηκε, η ηλεκτρονική υπογραφή είναι κυρίως μια νομική έννοια, επειδή έχει αναλυθεί. Ο όρος ψηφιακή υπογραφή χρησιμοποιείται μόνο για να περιγράψει την κατηγορία της ηλεκτρονικής υπογραφής που δημιουργήθηκε από τη μέθοδο της κρυπτογράφησης. (Bose & Vijayakumar, 2016)

Ως εκ τούτου, όσον αφορά τη μέθοδο δημιουργίας ηλεκτρονικής υπογραφής, μπορεί να συναχθεί το συμπέρασμα ότι αυτή είναι η πιο ασφαλής μέθοδος επαλήθευσης μιας «ηλεκτρονικής» ταυτότητας, διασφαλίζοντας την εμπιστευτικότητα του εγγράφου. Στην πραγματικότητα, όπως τόνισαν οι άνθρωποι, οι ψηφιακές υπογραφές μας επιτρέπουν να υπογράψουμε μηνύματα προκειμένου να εντοπίζουμε τυχόν αλλαγές στο περιεχόμενο του μηνύματος και να διασφαλίσουμε ότι ο αποστολέας δεν θα αρνηθεί ότι έστειλε ο ίδιος το μήνυμα. (Bose & Vijayakumar, 2016)

Τα ανοιχτά δίκτυα ηλεκτρονικής επικοινωνίας (όπως το Διαδίκτυο) είναι δίκτυα στα οποία μπορεί να συμμετέχει απεριόριστος αριθμός ατόμων. Στο ανοιχτό δίκτυο, επειδή οι άνθρωποι δεν γνωρίζουν ο ένας τον άλλον, η ζήτηση για υψηλή ασφάλεια και εμπιστευτικότητα πραγματοποιείται, και ως αποτέλεσμα, οι ηλεκτρονικές συναλλαγές δεν είναι ούτε αξιόπιστες ούτε ασφαλείς. Σε ένα κλειστό δίκτυο, οι ηλεκτρονικές



συναλλαγές μεταξύ ατόμων είναι ασφαλείς και αξιόπιστες. Αυτό συμβαίνει, επειδή μόνο λίγα άτομα μπορούν να συμμετάσχουν σε κλειστό δίκτυο. Μερικά από τα ζητήματα ασφαλείας που βλέπουμε στις συναλλαγές ηλεκτρονικού εμπορίου είναι (Καραδημητρίου, 2008):

Α) Παρακολούθηση γραμμών επικοινωνίας.

Β) Κατάχρηση/κλοπή κλειδιών πρόσβασης ή κωδικών πρόσβασης. Η παρακολούθηση των γραμμών επικοινωνίας είναι πολύ εύκολη και είναι επίσης πολύ εύκολη η καταγραφή και η κλοπή ηλεκτρονικών κλειδιών ή κωδικών πρόσβασης που χρησιμοποιούνται για την πρόσβαση σε στοιχεία ή αριθμούς πιστωτικών καρτών.

Γ) Παρακολούθηση και τροποποίηση των μεταδιδόμενων πληροφοριών.

Αυτό μπορεί να προκαλέσει σοβαρές οικονομικές απώλειες και ζημιές σε εμπορικές δραστηριότητες. Ένα παράδειγμα είναι ότι εάν ένας υποκλοπής διακόπτει την επικοινωνία μεταξύ ενός εμπόρου και ενός προμηθευτή σχετικά με μια παραγγελία για ένα ορισμένο ποσό αγαθών και τροποποιεί τις πληροφορίες, αυτό θα προκαλέσει τεράστιες οικονομικές απώλειες τόσο στον έμπορο όσο και στον προμηθευτή. Ένα άλλο παράδειγμα είναι όταν λέμε ότι πούλησα ένα αντικείμενο αξίας 1.000, και ο υποκλοπής τροποποίησε τις πληροφορίες έτσι ώστε να μπορέσει να βάλει όποια αξία ήθελε να προκαλέσει ζημιά στον ιδιοκτήτη του αντικειμένου, επειδή μπορούσε να γράψει 10 αντί 1.000.

Δ) Μεταμείωση μέσω ηλεκτρονικής πλαστογράφησης. Άτομα που χρησιμοποιούν ψεύτικες διευθύνσεις ηλεκτρονικού ταχυδρομείου και αναγνωριστικά ενδέχεται να εξαπατήσουν τους χρήστες σε συναλλαγές.

(Καραδημητρίου, 2008)

Η ηλεκτρονική υπογραφή είναι δεδομένα σε ηλεκτρονική μορφή, τα οποία συνδέονται λογικά με δεδομένα σε άλλες ηλεκτρονικές μορφές που αποδεικνύουν την αυθεντικότητά του. Αυτή η υπογραφή (ηλεκτρονική υπογραφή) μπορεί να παρέχει το ίδιο νομικό αποτέλεσμα με μια χειρόγραφη υπογραφή υπό ορισμένες προϋποθέσεις, αλλά η προϋπόθεση είναι ότι η υπογραφή πρέπει να πληρεί τις απαιτήσεις των ειδικών κανονισμών κάθε κράτους σχετικά με αυτό το θέμα. Η ασφαλέστερη και πιο αξιόπιστη



μέθοδος ηλεκτρονικής υπογραφής είναι η πλήρως αναγνωρισμένη μέθοδος χειρόγραφης υπογραφής. Το μεγαλύτερο πρόβλημα που απαιτεί η επιστήμη των υπολογιστών για επίλυση είναι η ασφάλεια των συναλλαγών χρησιμοποιώντας ηλεκτρονικές υπογραφές, επειδή οι κακόβουλοι χρήστες έχουν τη δυνατότητα να παρακολουθούν δεδομένα. Επομένως, υπάρχουν πολλοί τρόποι για να επιτρέψουμε σε κάποιον να πραγματοποιεί διαδικτυακές συναλλαγές, και είναι όλο και λιγότερο ασφαλής και ηλεκτρονικές υπογραφές μπορούν να χρησιμοποιηθούν για να δείξουν την πρόθεση των ηλεκτρονικών υπογραφών, του περιεχομένου του αρχείου ή της ταυτότητάς του. (Καραδημητρίου, 2008)

Παρακάτω αναφέρονται πολλοί απλοί αλλά ανασφαλείς τρόποι διεξαγωγής διαδικτυακών συναλλαγών:

1. Προσθέστε το όνομα του συντάκτη του εγγράφου στο τέλος του εγγράφου.
2. Χρησιμοποιήστε τη διεύθυνση email που χρησιμοποιείται από κάθε χρήστη.
3. Εικόνα υπογραφής χρήστη σε ψηφιακή μορφή.
4. Κάντε κλικ στο αντίστοιχο παράθυρο αποδοχής στην ιστοσελίδα για να αποδεχτείτε τους όρους που καθορίζονται από τον webmaster και απλώς να τον αποδεχτείτε.
5. Το ψηφιακό σήμα που χρησιμοποιείται από τον χρήστη ως υπογραφή.

(Καραδημητρίου, 2008)

Υπάρχει ένα κοινό. Είναι πολύ εύκολο να αντιγράψετε αυτές τις διάφορες υπογραφές και στη συνέχεια να τις χρησιμοποιήσετε για να βλάψετε ένα άτομο. Ως εκ τούτου, έχουν αναπτυχθεί διάφορες μέθοδοι για να διατηρείται η ηλεκτρονική υπογραφή ασφαλής. (Καραδημητρίου, 2008)

Μερικά από αυτά είναι: 1. Υπογραφή, η προϋπόθεση της οποίας είναι η γνώση του μοναδικού κώδικα. 2. Υπογραφή κρυπτογράφησης. 3. Υπογραφή με βιομετρικά χαρακτηριστικά. (Καραδημητρίου, 2008) Παρακάτω είναι μια εικόνα με

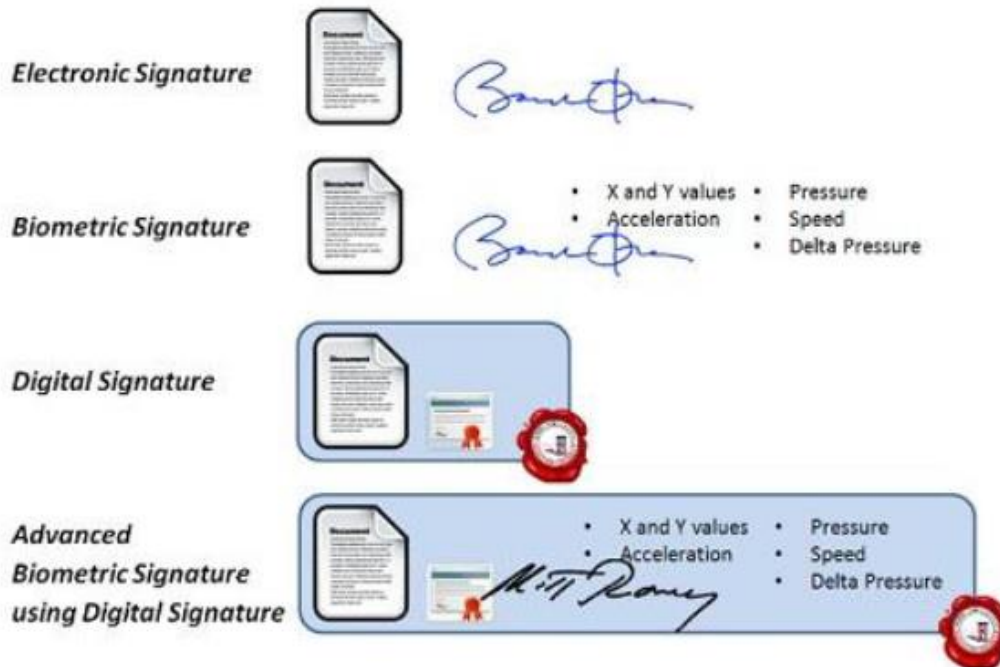


διαφορετικούς

τύπους

υπογραφών:

Signatures Types



Ο σκοπός της χρήσης ηλεκτρονικών υπογραφών είναι να παρέχει μια ασφαλή και ακριβή μέθοδο αναγνώρισης για τον υπογράφοντα, έτσι ώστε να είναι σε θέση να πραγματοποιεί ηλεκτρονικές συναλλαγές σε έναν προσομοιωμένο κόσμο. Ο ορισμός της ηλεκτρονικής υπογραφής ποικίλλει ανάλογα με τους ισχύοντες νόμους της χώρας / περιοχής ανταλλαγής. (Καραδημητρίου, 2008) Ωστόσο, υπάρχει ένας κοινός παρονομαστής. Απαιτήσεις για βασικές λειτουργίες, όπως:

- Η μοναδικότητα της αναγνώρισης ψηφιακής υπογραφής.
- Ο υπογράφων πρέπει να είναι το μόνο άτομο που έχει το δικαίωμα να χρησιμοποιεί την τεχνολογία παραγωγής υπογραφής.
- Τα δεδομένα πρέπει να παραμείνουν αμετάβλητα και εάν αλλάξει η υπογραφή θα ακυρωθεί.
- Η δημιουργημένη υπογραφή έχει υψηλότερο επίπεδο ασφάλειας.

Από τεχνική άποψη, οι ηλεκτρονικές υπογραφές με αποτελεσματική τεχνολογία πραγματοποιούνται χρησιμοποιώντας προηγμένες ηλεκτρονικές υπογραφές με



ψηφιακά πιστοποιητικά, τα οποία έχουν κρυπτογραφηθεί από μια ασφαλή συσκευή υπογραφής και έχουν πιστοποιηθεί από έναν εξειδικευμένο αξιόπιστο πάροχο υπηρεσιών. (Καραδημητρίου, 2008)



Η πιστοποίηση του ΠΥΠ για την έκδοση πιστοποιητικών γνησιότητας

Σύμφωνα με το άρθρο 3 του Προεδρικού Διατάγματος Αρ. 150/2001, οι προηγμένες ηλεκτρονικές υπογραφές που δημιουργούνται με ασύμμετρες κρυπτογραφικές μεθόδους θεωρούνται ισοδύναμες με χειρόγραφες υπογραφές. 150/2001, που ενσωματώθηκε στην ελληνική νομοθεσία σύμφωνα με το άρθρο 2, τμήμα 11, η οδηγία 99/93 του κώδικα των Ηνωμένων Πολιτειών, ορίζεται ως "φυσικό ή νομικό πρόσωπο ή άλλο ίδρυμα που εκδίδει πιστοποιητικά ή παρέχει υπηρεσίες που σχετίζονται με ηλεκτρονικές υπογραφές." Παρόλο που το «Πρόγραμμα συνεργατών» έχει καταστεί νομοθετικό μέτρο που εμποδίζει τους ανθρώπους να αμφισβητήσουν την ταυτότητα των ατόμων που ανταλλάσσουν ψηφιακά δεδομένα, εξακολουθούν να υπάρχουν ορισμένα προβλήματα στην επαλήθευση της ταυτότητας των ατόμων και του ίδιου του οργανισμού επαλήθευσης. Όταν χρησιμοποιούμε δημόσια κλειδιά για συναλλαγές, υπάρχει πρόβλημα ελέγχου ταυτότητας με τα ίδια τα κλειδιά, επειδή μπορούν να αναγνωριστούν ως ψηφιακά έγγραφα και πρέπει επίσης να έχουν την ψηφιακή υπογραφή του κατασκευαστή τους. (Ιγγλεζάκης, 2009)

Αυτό σημαίνει ότι η αρχή πιστοποίησης πρέπει να έχει ένα ζευγάρι κλειδιών κρυπτογράφησης και πρέπει επίσης να υποστηρίζεται από τα απαιτούμενα παρόμοια πιστοποιητικά δημόσιου κλειδιού και πρέπει να έχει ψηφιακή υπογραφή. Το παραπάνω πρόβλημα επιλύεται δημιουργώντας ένα αυτο-υπογεγραμμένο πιστοποιητικό, το οποίο δημιουργείται από τον βασικό εκδότη πιστοποιητικών ΠΥΠ, το οποίο ουσιαστικά αποτελεί τη βάση για τη δημιουργία ενός δημόσιου κλειδιού. Στην περίπτωση που ένα από τα ενδιάμεσα στάδια της υλοποίησης της αλυσίδας υπογραφών είναι αναξιόπιστο, η παραπάνω μέθοδος δεν είναι αρκετά αξιόπιστη επειδή έχει προβλήματα αξιοπιστίας, γεγονός που καθιστά ολόκληρη τη διαδικασία αναξιόπιστη. Σύμφωνα με τους νέους «κανονισμούς για την ηλεκτρονική αναγνώριση και τις υπηρεσίες εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά της ΕΕ» και την κατάργηση της οδηγίας 1999/93 / ΕΚ, ενέκρινε μια νέα μέθοδο εισαγωγής. Ουσιαστικά, δημιουργείται ένα "τρίτο μέρος" που ελέγχει το πιστοποιητικό. Το τρίτο είναι συνήθως ένα κράτος ή ένας κρατικός οργανισμός. (Ιγγλεζάκης, 2009)



Νομικά πλαίσια Ηλεκτρονικών εγγράφων και Ψηφιακών υπογραφών

Σε αυτό το κεφάλαιο, θα αναλύσουμε τους νόμους που ισχύουν για τις ηλεκτρονικές υπογραφές και τις διαδικαστικές απαιτήσεις που πρέπει να τηρούνται κατά τη συναλλαγή αυτών των εγγράφων. Συγκεκριμένα, θα δούμε το περιεχόμενο που ισχύει για πιστοποιητικά με ηλεκτρονικές υπογραφές και ηλεκτρονικά έγγραφα που ισχύουν για τους κανονισμούς 910/2014, θα δούμε τους νομικούς ορισμούς των απλών και προηγμένων ηλεκτρονικών εγγράφων υπογραφής και θα συζητήσουμε εγκεκριμένες υπογραφές και Πιστοποιητικά, συναφείς εμπιστευτικές υπηρεσίες και ευθύνες για εγκεκριμένες πιστωτικές υπηρεσίες.

Ο κανονισμός 910/2014 για τις ηλεκτρονικές υπογραφές

Αυτός ο κανονισμός τέθηκε σε ισχύ τον Ιούλιο του 2014 και περιλαμβάνει ηλεκτρονικές υπογραφές, ηλεκτρονικά γραμματόσημα, ηλεκτρονικά χρονικά σήματα, ηλεκτρονικά έγγραφα, υπηρεσίες παράδοσης ηλεκτρονικής εγγραφής και υπηρεσίες ελέγχου ταυτότητας πιστοποιητικών. Αυτά τα έγγραφα πρέπει να συμμορφώνονται με τις ακόλουθες διατάξεις στο άρθρο 910/2014 του κανονισμού (ΕΕ). Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της 23ης Ιουλίου 2014. (Δελούκα-Ιγγλέση, 2015)

Σύμφωνα με το άρθρο 26 του άρθρου 910/2014, η υπογραφή προηγμένων ηλεκτρονικών εγγράφων πρέπει να πληροί τις ακόλουθες προϋποθέσεις:

1. Να έχει την ικανότητα να συνδέεται με μοναδικό τρόπο με τον υπογράφοντα .
2. Να έχει την ικανότητα να ταυτοποιεί τον υπογράφοντα.
3. Δημιουργείται με ηλεκτρονικά δεδομένα δημιουργίας υπογραφών, ο υπογράφων μπορεί να χρησιμοποιήσει τα δεδομένα με μεγάλη εμπιστοσύνη υπό τον αποκλειστικό του έλεγχο.
4. Να μπορεί να πραγματοποιήσει την σύνδεση με τα υπογεγραμμένα δεδομένα που σχετίζονται με αυτό, ώστε να εντοπίζονται τυχόν μεταγενέστερες τροποποιήσεις σε αυτά τα δεδομένα

Τα εγκεκριμένα πιστοποιητικά ηλεκτρονικής υπογραφής περιέχουν:

1. Μια ένδειξη, μια οδηγία σε μορφή κατάλληλη για αυτόματη επεξεργασία, που δείχνει ότι το πιστοποιητικό έχει εκδοθεί ως εγκεκριμένο ηλεκτρονικό πιστοποιητικό υπογραφής.



2. Ένα σύνολο δεδομένων που δηλώνει με σαφήνεια τον εγκεκριμένο αξιόπιστο πάροχο υπηρεσιών που έχει εκδώσει το πιστοποιητικό έγκρισης, συμπεριλαμβανομένης τουλάχιστον της χώρας μέλους που δημιούργησε το πιστοποιητικό, και (εάν ένα νομικό πρόσωπο): όνομα και αριθμός εγγραφής (εάν ισχύει) όπως αναφέρεται στα επίσημα αρχεία, -Για φυσικά πρόσωπα: το όνομα του ατόμου
3. Το όνομα του υπογράφοντος ή ένα ψευδώνυμο εάν το οποίο, είναι απαραίτητο να αναφέρεται με πλήρη σαφήνεια.
4. Τα δεδομένα επαλήθευσης ηλεκτρονικής υπογραφής τα οποία αντιστοιχούν στα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής
5. Λεπτομέρειες σχετικά με την έναρξη και το τέλος της περιόδου ισχύος του πιστοποιητικού.
6. Το αναγνωριστικό του πιστοποιητικού, το οποίο πρέπει να είναι μοναδικό για τον εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης.
7. Η προηγμένη ηλεκτρονική υπογραφή ή η προηγμένη ηλεκτρονική σφραγίδα του εγκεκριμένου εκδότη παρέχει υπηρεσίες εμπιστοσύνης.
8. Ένας ιστότοπος που παρέχει πιστοποιητικό που αποδεικνύει δωρεάν ηλεκτρονική υπογραφή ή προηγμένη ηλεκτρονική σφραγίδα που αναφέρεται στο έργο δωρεάν.
9. Τοποθεσίες υπηρεσίας που μπορούν να χρησιμοποιηθούν για τη λήψη πληροφοριών σχετικά με την εγκυρότητα των εγκεκριμένων πιστοποιητικών.
10. Στην περίπτωση που τα δεδομένα δημιουργίας υπογραφής που σχετίζονται με τα δεδομένα επιβεβαίωσης ηλεκτρονικής υπογραφής βρίσκονται στην εγκεκριμένη ηλεκτρονική συσκευή δημιουργίας υπογραφών, η κατάλληλη οδηγία είναι τουλάχιστον σε μορφή κατάλληλη για αυτόματη επεξεργασία.
(Δελούκα-Ιγγλέση, 2015)

Επίσης, σύμφωνα με τις ίδιες νομικές διατάξεις, καθορίζονται οι απαιτήσεις των εγκεκριμένων διατάξεων για τη δημιουργία ηλεκτρονικών υπογραφών:

Ο εγκεκριμένος εξοπλισμός ηλεκτρονικής υπογραφής θα πρέπει τουλάχιστον να διασφαλίζεται με κατάλληλα τεχνικά και διαδικαστικά μέσα:



α) Η εμπιστευτικότητα των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιούνται για τη δημιουργία της ηλεκτρονικής υπογραφής διασφαλίζεται εύλογα.

β) Τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής μπορούν να εμφανίζονται μόνο μία φορά στην πράξη

γ) Χωρίς εύλογη διαβεβαίωση, η ηλεκτρονική υπογραφή δεν μπορεί να προκύψει για τη δημιουργία δεδομένων και η τρέχουσα τεχνολογία δεν μπορεί να χρησιμοποιηθεί για την αξιόπιστη προστασία της ηλεκτρονικής υπογραφής από πλαστογράφηση.

δ) Οι νόμιμοι υπογράφοντες μπορούν να προστατεύσουν αξιόπιστα τα δεδομένα δημιουργίας ηλεκτρονικών υπογραφών για να αποτρέψουν τη χρήση τρίτων

(Δελούκα-Ιγγλέση, 2015)

1. Η εγκεκριμένη δημιουργία ηλεκτρονικών υπογραφών δεν αλλάζει τα προς υπογραφή δεδομένα, ούτε εμποδίζει την υποβολή αυτών των δεδομένων στον υπογράφοντα πριν την υπογραφή.
2. Η δημιουργία ή η διαχείριση των δεδομένων δημιουργίας υπογραφής από τον υπογράφοντα μπορεί να πραγματοποιηθεί μόνο από εξουσιοδοτημένο πάροχο υπηρεσιών εμπιστοσύνης.
3. Με την επιφύλαξη του σημείου 1 στοιχείο
4. Ο εξουσιοδοτημένος αξιόπιστος πάροχος υπηρεσιών που διαχειρίζεται τα δεδομένα δημιουργίας υπογραφής από τον υπογράφοντα μπορεί να αντιγράψει τα δεδομένα δημιουργίας υπογραφών μόνο για σκοπούς δημιουργίας αντιγράφων ασφαλείας, εφόσον πληρούνται οι ακόλουθες προϋποθέσεις (Δελούκα-Ιγγλέση, 2015):

α) Η ασφάλεια των αντιγραμμένων δεδομένων είναι στο ίδιο επίπεδο με την ασφάλεια των αρχικών δεδομένων,

β) Ο αριθμός των επαναλαμβανόμενων συνόλων δεδομένων δεν υπερβαίνει τον ελάχιστο απαιτούμενο αριθμό για να εξασφαλιστεί η συνέχεια της υπηρεσίας.

(Δελούκα-Ιγγλέση, 2015)



Εγκεκριμένες ηλεκτρονικές υπογραφές

Σύμφωνα με το άρθρο 3 παράγραφος 12 του νόμου 910/2014 που ορίζεται από την Ευρωπαϊκή Ένωση, μια εγκεκριμένη ηλεκτρονική υπογραφή είναι μια προηγμένη ηλεκτρονική υπογραφή που δημιουργήθηκε από μια εγκεκριμένη συσκευή δημιουργίας ηλεκτρονικών υπογραφών, η οποία βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής. Αυτό σημαίνει ότι τέτοιες υπογραφές πρέπει να έχουν τα ίδια στοιχεία με τις προηγμένες ηλεκτρονικές υπογραφές και πρέπει να δημιουργούνται από εγκεκριμένες συσκευές. Η εγκεκριμένη ηλεκτρονική υπογραφή έχει το νομικό αποτέλεσμα ισοδύναμο με αυτό μιας χειρόγραφης υπογραφής. (Δελούκα-Ιγγλέση, 2015)

Τα εγκεκριμένα πιστοποιητικά ηλεκτρονικής υπογραφής εκδίδονται από παρόχους (δημόσιο και ιδιωτικό) και έχουν εγκριθεί ειδικά από την εθνική αρμόδια αρχή, όπως φαίνεται στους εθνικούς μυστικούς καταλόγους των κρατών μελών της ΕΕ, στους οποίους μπορείτε να έχετε πρόσβαση μέσω αξιόπιστων προγραμμάτων περιήγησης. Πολλοί πάροχοι πιστοποίησης παραδίδουν το αντίστοιχο ιδιωτικό κλειδί σε μια γεννήτρια ειδικής υπογραφής. Παρόλο που ενδέχεται να απαιτούνται διαφορετικά επίπεδα ηλεκτρονικών υπογραφών υπό διαφορετικές συνθήκες, μόνο σε ολόκληρη την Ευρωπαϊκή Ένωση μπορούν τα έγγραφα ηλεκτρονικής υπογραφής που έχουν το ίδιο νομικό αποτέλεσμα με τις χειρόγραφες υπογραφές. (Δελούκα-Ιγγλέση, 2015)

Εγκεκριμένα πιστοποιητικά

Το εγκεκριμένα πιστοποιητικά είναι ένας κατάλογος αξιόπιστων πιστοποιητικών εγκεκριμένων από τη χώρα (ειδικά η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων της Ελλάδας). Σύμφωνα με το νόμο 910/2014 της Ευρωπαϊκής Ένωσης για τα ηλεκτρονικά έγγραφα και τις ηλεκτρονικές υπογραφές, η Πολιτεία της Νέας Υόρκης θα εγκρίνει αυτούς τους παρόχους πιστοποιητικών. Κάποιος μπορεί να δει την λίστα στον σύνδεσμο αυτόν" Η απόφαση 2009/767 / ΕΚ της Επιτροπής στις 16 Οκτωβρίου 2009 προωθεί τη διασυννοριακή χρήση ηλεκτρονικών υπογραφών. Το ψήφισμα απαιτεί από τα κράτη μέλη να διατυπώσουν, να διατηρήσουν και να δημοσιεύσουν έναν κατάλογο αξιόπιστων πληροφοριών σχετικά με πιστοποιητικά που εκδίδονται από παρόχους υπηρεσιών πιστοποιητικών και συμμορφώνεται με την Ευρωπαϊκή Οδηγία 1999/93 / ΕΚ. Οι πληροφορίες σχετικά με το πλαίσιο της



κοινότητας ηλεκτρονικών υπογραφών που εκδόθηκαν από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο στις 13 Δεκεμβρίου 1999 υπόκεινται σε εποπτεία από τα κράτη μέλη. Ο τρέχων αξιόπιστος κατάλογος αποτελεί συνέχεια του εμπιστευτικού καταλόγου που καταρτίστηκε με την απόφαση 2009/767 / ΕΚ. Το ισχύον νομικό πλαίσιο για αυτόν τον εμπιστευτικό κατάλογο είναι ο κανονισμός της ΕΕ αριθ. 182/2011. (Δελούκα-Ιγγλέση, 2015)

Ο κανονισμός (ΕΚ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με τις υπηρεσίες ηλεκτρονικής αναγνώρισης και αξιοπιστίας για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και καταργεί την οδηγία 1999/93 / ΕΚ. Επομένως, τα άτομα που θα χρησιμοποιήσουν το πιστοποιητικό πρέπει να αναφέρονται σύμφωνα με τους ισχύοντες νόμους. (Δελούκα-Ιγγλέση, 2015)

Ωστόσο, μπορούμε να δούμε ένα είδος πιστοποιητικού X.509, το οποίο αρχικά εκδόθηκε στις 3 Ιουλίου 1988 και ξεκίνησε σε συνεργασία με το πρότυπο X.500. Στην πραγματικότητα, ο όρος "πιστοποιητικό X.509" αναφέρεται συνήθως στο IET RKIX, το πιστοποιητικό και το αρχείο διαμόρφωσης ΚΕΑ του τυπικού πιστοποιητικού X 509 3 που ορίζεται στο RFC 5280. Εδώ, αναφέρεται στην υποδομή δημόσιου κλειδιού X509. Η δομή του X.509 v3 έχει ως εξής:

- Πιστοποιητικό
- Ο Εκδοχή
- Αύξων αριθμός
- Αλγόριθμος ID ο Εκδότης
- Εγκυρότητα
 - Πριν από όχι
 - Μετά δεν
- Θέμα
 - Αλγόριθμος δημόσιου κλειδιού
 - Θέμα Public Key
- Εκδότη μοναδικό αναγνωριστικό (Προαιρετικό)



- Θέμα μοναδικό αναγνωριστικό (Προαιρετικό)
- Extensions (Προαιρετικό)
 - Πιστοποιητικό Αλγόριθμος Υπογραφή
 - Πιστοποιητικό Υπογραφή

Χρήση του πιστοποιητικού:

- ✓ Η χρήση του κλειδιού χρησιμοποιείται για τον προσδιορισμό της χρήσης του δημόσιου κλειδιού που περιέχεται στο πιστοποιητικό.
- ✓ Η επέκταση κλειδιού χρησιμοποιείται για να δείξει τον σκοπό του δημόσιου κλειδιού που περιέχεται στο πιστοποιητικό,
- ✓ Οι βασικοί περιορισμοί χρησιμοποιούνται για να δείξουν ότι το πιστοποιητικό ανήκει στην ΑΠ.

Το RFC 5230 δηλώνει ότι δύο πιστοποιητικά πρέπει να υποβάλλονται σε επεξεργασία ταυτόχρονα και το πιστοποιητικό μπορεί να χρησιμοποιηθεί μόνο όταν οι δύο επεκτάσεις είναι συνεπείς στη χρήση του καθορισμένου πιστοποιητικού. (Δελούκα-Ιγγλέση, 2015)

Υπηρεσίες εμπιστοσύνης

Εγκεκριμένες ή αλλιώς εξειδικευμένες υπηρεσίες εμπιστοσύνης είναι υπηρεσίες εμπιστοσύνης που συμμορφώνονται με τους κανονισμούς που ορίζονται στον Κανονισμό 910/2014. Για έλεγχο, υπάρχει εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης. Σύμφωνα με τους κανονισμούς, ο πάροχος ορίζεται ως πάροχος υπηρεσιών εμπιστοσύνης που παρέχει μία ή περισσότερες εγκεκριμένες υπηρεσίες εμπιστοσύνης και έχει εγκριθεί από τον ρυθμιστικό φορέα μέσω του ίδιου εγγράφου. Αυτές οι υπηρεσίες υποχρεούνται να συμμορφώνονται με τους κανονισμούς καθ' όλη τη διαδικασία παροχής υπηρεσιών και να ελέγχονται κάθε δύο χρόνια σύμφωνα με τους κανονισμούς με δικά σας έξοδα. (Δελούκα-Ιγγλέση, 2015)

Σύμφωνα με την απόφαση του κανονισμού αριθ. 910/2014, η Επιτροπή αποφάσισε να δημιουργήσει μια υπηρεσία εμπιστοσύνης που θα λειτουργεί ως "κατασκευαστής" ηλεκτρονικών υπογραφών, δηλαδή θα είναι υπεύθυνη για τη δημιουργία, τον έλεγχο, την επαλήθευση, την επεξεργασία και τη συντήρηση. Υπάρχουν δύο τύποι υπηρεσιών: εγκεκριμένες υπηρεσίες και μη εγκεκριμένες υπηρεσίες. Στο επόμενο κεφάλαιο, θα



αναφερθούμε σε εγκεκριμένες υπηρεσίες εμπιστοσύνης. Η ισχύς της νέας πρότασης είναι ίδια με τη μέθοδο του καταλόγου που αναφέρεται στην προηγούμενη μέθοδο. (Δελούκα-Ιγγλέση, 2015)

Ο νόμος ορίζει έναν πάροχο υπηρεσιών εμπιστοσύνης ως "φυσικό ή νομικό πρόσωπο που παρέχει μία ή περισσότερες υπηρεσίες εμπιστοσύνης ως εγκεκριμένο ή μη εξουσιοδοτημένο πάροχο υπηρεσιών εμπιστοσύνης".

Επίσης, σύμφωνα με το ίδιο νομικό έγγραφο, το άρθρο 3, παράγραφος 16, ορίζει τις υπηρεσίες εμπιστοσύνης ως ηλεκτρονικές υπηρεσίες που συνήθως απαιτούν πληρωμή, συμπεριλαμβανομένων:

α) Κατά τη δημιουργία, επαλήθευση και επιβεβαίωση ηλεκτρονικών υπογραφών, ηλεκτρονικών σφραγίδων ή ηλεκτρονικών χρονοσήμων, ηλεκτρονικών υπηρεσιών παράδοσης εγγραφής και πιστοποιητικών που σχετίζονται με αυτές τις υπηρεσίες.

β) Κατά τη δημιουργία, επαλήθευση και επικύρωση πιστοποιητικών που χρησιμοποιούνται για την επαλήθευση της ταυτότητας του ισότοπου,

γ) κατά την προστασία ηλεκτρονικών υπογραφών, σφραγίδων ή πιστοποιητικών τα οποία σχετίζονται με αυτές τις υπηρεσίες

Σε περίπτωση παραβίασης της ασφάλειας, το τμήμα σέρβις υποχρεούται να ειδοποιεί τον νόμιμο εκπρόσωπο που εμπλέκεται στο ηλεκτρονικό αρχείο και να ενημερώνει το κοινό εάν εμπλέκονται πολλά αρχεία.

Ευθύνη εγκεκριμένων παρόχων

Σύμφωνα με το νόμο, οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης πρέπει να φέρουν ορισμένες ευθύνες, όπως ορίζονται στο άρθρο 24 του κανονισμού αριθ. προσδιορίστηκαν οι ακόλουθες απαιτήσεις:

Κατά την έκδοση πιστοποιητικού έγκρισης για υπηρεσίες εμπιστοσύνης, ο εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης επαληθεύει την ταυτότητα του φυσικού ή νομικού προσώπου που εκδίδει το πιστοποιητικό έγκρισης μέσω κατάλληλων μεθόδων και σύμφωνα με την εθνική νομοθεσία, και επαληθεύει τα



φυσικά χαρακτηριστικά ή τυχόν ειδικά χαρακτηριστικά του υπό κατάλληλες συνθήκες χαρακτηριστικού.

1. Οι πληροφορίες οι οποίες αναφέρονται στο πρώτο εδάφιο επαληθεύονται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης απευθείας ή μέσω τρίτου σύμφωνα με την εθνική νομοθεσία:

α) Με φυσική παρουσία του προσώπου ή αλλιώς με εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου.

β) Από απόσταση, με τη χρήση μέσων ηλεκτρονικής ταυτοποίησης για τα οποία, πριν από την έκδοση του πιστοποιητικού έγκρισης, έχει διασφαλίσει τη φυσική ύπαρξη του φυσικού προσώπου ή του εξουσιοδοτημένου αντιπροσώπου του και έχει εκπληρώσει τις «βασικές» απαιτήσεις του άρθρου 8 για την απομακρυσμένη χρήση μεθόδων ηλεκτρονικής αναγνώρισης ή «υψηλού» επιπέδου διασφάλισης.

γ) Χρησιμοποιώντας εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής ή εγκεκριμένη ηλεκτρονική σφραγίδα που εκδίδεται σύμφωνα με τα στοιχεία (α) ή (β) ή (δ), χρησιμοποιώντας μια μέθοδο αναγνώρισης που αναγνωρίζεται από άλλες χώρες που παρέχει ισοδύναμη με την πραγματική εγγύηση, η ισοδύναμη εγγύηση επιβεβαιώνεται από τον οργανισμό αξιολόγησης.

2. Οι εγκεκριμένοι πάροχοι υπηρεσιών που παρέχουν εγκεκριμένες υπηρεσίες εμπιστοσύνης:

α) να ενημερώνουν τον ρυθμιστή για τυχόν αλλαγές στην παροχή υπηρεσιών εμπιστοσύνης που έχει εγκριθεί από αυτήν, συμπεριλαμβανομένης της πρόθεσης να σταματήσετε τέτοιες δραστηριότητες

β) να απασχολούν υπαλλήλους που διαθέτουν την απαραίτητη εμπειρογγνωμοσύνη, αξιοπιστία, εμπειρία και προσόντα και έχουν λάβει κατάλληλη εκπαίδευση σχετικά με τους κανόνες ασφάλειας και προστασίας δεδομένων, καθώς και υπερβολάβους, όπου απαιτείται, και εφαρμόζουν διοικητικές και διαχειριστικές διαδικασίες που πληρούν ευρωπαϊκά ή διεθνή πρότυπα.



γ) Όσον αφορά την ευθύνη για ζημίες που αναλαμβάνονται βάσει του άρθρου 13, σύμφωνα με την εθνική νομοθεσία, τη διατήρηση επαρκών οικονομικών πόρων ή και την εξασφάλιση επαρκούς ασφάλισης,

δ) Πριν από τη σύναψη συμβατικής σχέσης, θα πρέπει να ενημερώνουν με σαφήνεια και πληρότητα σε οποιονδήποτε επιθυμεί να χρησιμοποιήσει την εγκεκριμένη υπηρεσία εμπιστοσύνης για τους ακριβείς όρους και προϋποθέσεις χρήσης της υπηρεσίας, συμπεριλαμβανομένων των περιορισμών χρήσης.

ε) Να χρησιμοποιούν αξιόπιστα συστήματα και προϊόντα. Αυτά τα συστήματα και προϊόντα πρέπει να προστατεύονται από αλλαγές και να διασφαλίζουν την τεχνική ασφάλεια και αξιοπιστία των διαδικασιών που υποστηρίζουν.

στ) Να χρησιμοποιούν ένα αξιόπιστο σύστημα για την αποθήκευση των δεδομένων που τους παρέχονται σε επαληθεύσιμη μορφή, έτσι ώστε: 1) Μπορούν να εξαχθούν δημόσια μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων 2) εισαγωγή και τροποποίηση των αποθηκευμένων δεδομένων, (3) τα δεδομένα μπορούν να επαληθευτούν -Αυθεντικότητα-. Να ληφθούν τα κατάλληλα μέτρα για την πρόληψη της πλαστογράφησης και της κλοπής δεδομένων.

η) Ακόμη και μετά τη διακοπή των δραστηριοτήτων του εγκεκριμένου παρόχου υπηρεσιών εμπιστοσύνης, είναι απαραίτητο να καταγραφθεί και να διατηρηθεί η προσβασιμότητα εντός κατάλληλου χρόνου. Όλες οι σχετικές πληροφορίες που σχετίζονται με τα δεδομένα που δημοσιεύονται και λαμβάνονται από εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης, ιδίως παρέχοντας αποδεικτικά στοιχεία σε νομικές διαδικασίες και διασφαλίζοντας τη συνέχεια των υπηρεσιών, μπορούν να καταγραφούν ηλεκτρονικά.

Ανάπτυξη ενημερωμένου προγράμματος τερματισμού για τη διασφάλιση της συνέχειας της παροχής υπηρεσιών σύμφωνα με την αναθεώρηση του άρθρου 17 παράγραφος 4 σημείο 0 από την εποπτική αρχή. Διασφάλιση της νόμιμης επεξεργασίας δεδομένων προσωπικού χαρακτήρα σύμφωνα με την οδηγία 95/46 / ΕΚ



ι) Για εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης, εάν δημοσιεύουν εγκεκριμένα πιστοποιητικά τώρα, δημιουργήστε μια βάση δεδομένων πιστοποιητικών και διατηρήστε την ενημερωμένη.

3. Όταν ο εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης που εξέδωσε το πιστοποιητικό έγκρισης αποφασίζει να ανακαλέσει το πιστοποιητικό, καταγράφει την ανάκληση στη βάση δεδομένων πιστοποιητικών και σε κάθε περίπτωση, εκδίδει την ανάκληση του πιστοποιητικού εγκαίρως εντός 24 ωρών από την παραλαβή της αίτησης. Η ανάκληση παράγει αποτελέσματα αμέσως μετά την έκδοσή της.
4. Όσον αφορά την παράγραφο 3, ο εξουσιοδοτημένος πάροχος υπηρεσιών εμπιστοσύνης που εξέδωσε το πιστοποιητικό έγκρισης παρέχει σε κάθε μετεγκατεστημένο μέρος πληροφορίες σχετικά με την εγκυρότητα ή την ανάκληση του πιστοποιητικού έγκρισης που εκδίδει. Τουλάχιστον σε κάθε πιστοποιητικό, εντός της περιόδου ισχύος του πιστοποιητικού, αυτές οι πληροφορίες μπορούν να ληφθούν με αξιόπιστο, δωρεάν και αποτελεσματικό αυτοματοποιημένο τρόπο, τουλάχιστον κάθε φορά.
5. Η επιτροπή μπορεί να καθορίσει τυποποιημένους αριθμούς αναφοράς για αξιόπιστα συστήματα και προϊόντα που πληρούν τις απαιτήσεις της παραγράφου 2 στοιχεία ε) και στ) του παρόντος άρθρου μέσω εργασιών αξιολόγησης. Εάν αξιόπιστα συστήματα και προϊόντα πληρούν τα απαιτούμενα πρότυπα, θεωρείται ότι συμμορφώνονται με τις διατάξεις του παρόντος άρθρου.

Η εφαρμογή του Κανονισμού 910/2014 στην Ελλάδα

Η οικοδόμηση εμπιστοσύνης στο διαδικτυακό περιβάλλον είναι το κλειδί για την οικονομική και κοινωνική ανάπτυξη. Η έλλειψη εμπιστοσύνης, ιδίως λόγω της αναμφισβήτητης έλλειψης ασφάλειας δικαίου, καθιστά τους καταναλωτές, τις επιχειρήσεις και τους δημόσιους οργανισμούς απρόθυμους να πραγματοποιούν ηλεκτρονικές συναλλαγές και να υιοθετούν νέες υπηρεσίες. Στην Ελλάδα, υπήρχε πρόβλημα ορισμού πριν από τον κανονισμό 910/2014, το οποίο είχε ως αποτέλεσμα προβλήματα με συναλλαγές, με ηλεκτρονικές υπογραφές και ηλεκτρονικά έγγραφα (Δελούκα-Ιγγλέση, 2015).



Επομένως, ο κανονισμός αριθ. 910/2014 στοχεύει στην αύξηση της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά παρέχοντας μια κοινή βάση για ασφαλή ηλεκτρονική αλληλεπίδραση μεταξύ πολιτών, επιχειρήσεων και δημόσιων ιδρυμάτων, ενισχύοντας έτσι τις δημόσιες και ιδιωτικές ηλεκτρονικές υπηρεσίες, τις ηλεκτρονικές επιχειρήσεις και Ηλεκτρονική Αποδοτικότητα Εμπόριο ΕΕ. Με βάση το περιεχόμενο που αναλύσαμε στα προηγούμενα κεφάλαια, μπορούμε εύκολα να δούμε ότι ο νέος κανονισμός 910/2014 έχει υποστεί ειδικές αλλαγές και ότι έχουν αλλάξει οι κανονισμοί για την παροχή ηλεκτρονικών εγγράφων και κανονισμών ηλεκτρονικής υπογραφής και έχουν οριστεί νέοι ορισμοί για ενημέρωση. Είναι ιδιαίτερα σημαντικοί οι αλλαγές να γίνουν σε ηλεκτρονικές υπογραφές που έχουν νομική ισχύ και να αντικαθιστούν χειρόγραφες ή πιο ρητές ηλεκτρονικές υπογραφές και τις υποστηρίζουν επειδή δεν τις έχουν καταργήσει.

Κατ' αρχήν, η θέση της χειρόγραφης υπογραφής αντικαθίσταται τώρα από εγκεκριμένη ηλεκτρονική υπογραφή. Επιπλέον, αξιόπιστοι πάροχοι υπηρεσιών που ενδιαφέρονται να παρέχουν εγκεκριμένες αξιόπιστες υπηρεσίες θα πρέπει να επικοινωνήσουν με την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ). Η ΕΕΤΤ, ορίστηκε ως αρμόδια αρχή υπεύθυνη για την έγκριση παροχών εμπιστοσύνης. Επομένως, οι υπηρεσίες εμπιστοσύνης πρέπει να υποβάλουν αίτηση για έγκριση στην ΕΕΤΤ. Μια ιδιαίτερα σημαντική αλλαγή είναι ο πιο σωστός ορισμός των προηγμένων ηλεκτρονικών υπογραφών, διότι έχει πλέον αποκτήσει σαφή κατάσταση και δεν περιορίζεται στον ορισμό των ψηφιακών υπογραφών που έγιναν σε προηγούμενους κανονισμούς (Δελούκα-Ιγγλέση, 2015).

Συγκεκριμένα, οι πάροχοι που εκδίδουν πιστοποιητικά έγκρισης σύμφωνα με την οδηγία 1999/93 / ΕΚ, δηλαδή το Π.Δ. 150/2001, υποβάλλουν εκθέσεις αξιολόγησης της συμμόρφωσης στον ρυθμιστικό οργανισμό το συντομότερο δυνατό και το αργότερο την 1η Ιουλίου 2017, έως ότου υποβληθούν οι εκθέσεις αξιολόγησης της συμμόρφωσης και μέχρι την ολοκλήρωση της αξιολόγησης από τον ρυθμιστικό οργανισμό, οι νέοι κανονισμοί. Σύμφωνα με τους κανονισμούς της 2ης Ιουλίου 2017, εάν δεν υποβάλουν την έκθεση αξιολόγησης της συμμόρφωσης στην ΕΕΤΤ εντός της προθεσμίας, αυτοί οι πάροχοι δεν θα θεωρηθούν εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης.



Επιπλέον, η ΕΕΤΤ διατηρεί μητρώο εγκεκριμένων και μη εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης που είναι εγκατεστημένοι στην Ελλάδα. Όσον αφορά τον ορισμό της προηγμένης ηλεκτρονικής υπογραφής, δεν προσδιορίζεται μόνο από την ψηφιακή υπογραφή, επομένως το νόημά της δεν περιορίζεται, όπως έκανε και το προηγούμενο Προεδρικό Διάταγμα 150/2001. Επιπλέον, το κύριο σημείο του νέου κανονισμού 910/2014 που έχει πρακτική εφαρμογή στην ελληνική νομοθεσία είναι το άρθρο 25.

Αυτό το άρθρο ορίζει ότι τα κράτη μέλη μεριμνούν, ώστε οι ηλεκτρονικές υπογραφές να μην απορρίπτονται σε νομικές διαδικασίες ως αποδεικτικά στοιχεία ως προς τη νομιμότητα και το παραδεκτό, δηλαδή όχι μόνο στα δικαστήρια αλλά και σε άλλα θεσμικά όργανα (όπως διαιτητές, διοικητικές υπηρεσίες) και βραβεία. Προσφυγή σε πειθαρχικές υπηρεσίες, επαγγελματικές ενώσεις και ακόμη και συνδικάτα. Τέλος, ο κοινοτικός νομοθέτης ρύθμισε τη λειτουργία ηλεκτρονικών υπογραφών σε δημόσιες υπηρεσίες.

Επιπλέον, όσον αφορά την αποδεικτική αξία των ηλεκτρονικών στην Ελλάδα, σύμφωνα με τον κανονισμό 910/2014 πολλές δικαστικές αποφάσεις επεσήμαναν ότι στην περίπτωση που οι διάδικοι δεν ορίζουν τη συμμόρφωση με τη γραπτή μορφή (άρθρο 160 του Αστικού Κώδικα), αρκεί μια απλή ηλεκτρονική υπογραφή. Στην πραγματικότητα, σε αυτήν την περίπτωση, θα πρέπει να σας υπενθυμίσουμε ότι για να θεωρηθεί έγκυρη μια απλή ηλεκτρονική υπογραφή και να δοθεί επαρκής απόδειξη σε μια μηχανική παράσταση, πρέπει να αποδειχθεί ότι μπορεί να λειτουργήσει ως «ηλεκτρονικό υποκατάστατο των προσωπικών υπογραφών». Με βάση τα παραπάνω αποτελέσματα της έρευνας, αξίζει να αναφερθούν λεπτομερέστερα οι πιο συγκεκριμένες μορφές απλών ηλεκτρονικών υπογραφών που γίνονται δεκτές από τη νομολογία, δηλαδή είναι αποδεκτές σε ορισμένες περιπτώσεις που συμμορφώνονται με το άρθρο 445 του Διεθνούς Συμφώνου για την Πολιτική και αξίωση πολιτικών δικαιωμάτων.

Η πιο συνηθισμένη περίπτωση μιας απλής ηλεκτρονικής υπογραφής είναι μια μοναδική διεύθυνση email για κάθε χρήστη. Συγκεκριμένα, ορισμένοι πιστεύουν ότι, εκτός από τη σύνδεση με τον αποστολέα και τη χρήση ειδικού κωδικού, η μέθοδος επικοινωνίας στο Διαδίκτυο με βάση το ηλεκτρονικό ταχυδρομείο απαιτεί τη λειτουργία του



ηλεκτρονικού ταχυδρομείου, με βάση την αναγνώριση του χρήστη στο σύστημα ως ο αποστολέας του e-mail ή του παραλήπτη.

Ο κωδικός είναι η διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη επειδή διατυπώνεται από τον χρήστη με τον αρχικό τρόπο χρησιμοποιώντας τους χαρακτήρες που επιλέγει, οι χαρακτήρες συνδυάζονται με τα σύμβολα και συνδυάζονται με τους χαρακτήρες που ορίζει ο προωθητής με αυτόν τον τρόπο. Ειδικοί συνδυασμοί χαρακτήρων ισχύουν μόνο για χρήστες που έχουν ορίσει τον χαρακτήρα και δεν μπορούν να χρησιμοποιηθούν νόμιμα από άλλους. Η εμφάνιση της διεύθυνσης του αποστολέα στο μήνυμα το καθιστά εντελώς ειδικό για τον παραλήπτη, οπότε δεν μπορεί να συγχέεται με άλλο χρήστη του ίδιου συστήματος, αν και είναι αδιαχώριστο από την ταυτότητα του περιεχομένου του μηνύματος.

Φυσικά, είναι βέβαιο ότι αυτό το μήνυμα μπορεί να έχει σταλεί από κάποιον άλλο από το άτομο στο οποίο ανήκει η συγκεκριμένη διεύθυνση ηλεκτρονικού ταχυδρομείου και χρησιμοποιήθηκε (με οποιονδήποτε τρόπο) χωρίς την άδειά του. Λαμβάνοντας υπόψη τα ανωτέρω, ο αντίκτυπος του άρθρου 457, παράγραφος 4 της Ευρωπαϊκής Σύμβασης για τα Ανθρώπινα Δικαιώματα περιορίζεται ουσιαστικά στον προσδιορισμό του περιεχομένου του σκληρού δίσκου του υπολογιστή και της μηχανικής του οθόνης.

Συνολικά, λαμβάνοντας υπόψη τη θέση της νομολογίας σε ηλεκτρονικά έγγραφα που θεωρείται ότι έχουν υπογραφεί, μπορεί κανείς να επιστρέψει στα αρχικά θεωρητικά ευρήματα σχετικά με τις νομικές συνέπειες των κατηγοριών ηλεκτρονικών υπογραφών. Ειδικότερα, όσον αφορά τις εγκεκριμένες ηλεκτρονικές υπογραφές (που αναγνωρίζονται βάσει του προηγούμενου νόμου), θεωρούνται οι μοναδικοί συνιδιοκτήτες αυτών των στοιχείων, οι οποίες έχουν όλες τις νομικές συνέπειες και στους δύο ουσιαστικούς αστικούς νόμους (άρθρο 160 του Αστικού Κώδικα) και διαδικαστικούς νόμους (ενότητα 445 Κώδικας Πολιτικής Οικονομίας (ΚΠολΔ)).

Ηλεκτρονικές συμβάσεις

Σύμφωνα με το νόμο 4761/2020 «Ως ηλεκτρονικό έγγραφο ορίζεται οποιοδήποτε περιεχόμενο έχει αποθηκευτεί σε ηλεκτρονική μορφή και ειδικότερα ως κείμενο ή με ηχητική, οπτική ή οπτικοακουστική εγγραφή».



Με την ταχεία ανάπτυξη του εμπορίου και τη νέα κατάσταση της διεθνούς οικονομίας, η ζήτηση για ηλεκτρονικές συμβάσεις έχει αυξηθεί. Η έννοια των ηλεκτρονικών μέσων δεν πρέπει να περιορίζεται στις τρέχουσες τεχνολογικές εξελίξεις (υπολογιστής και οποιαδήποτε μηχανική υποστήριξη). Ωστόσο, όλα τα επιτεύγματα με βάση τις ηλεκτρονικές υπηρεσίες και την περαιτέρω υποστήριξή τους μπορούν να θεωρηθούν ως ηλεκτρονικά μέσα. Ουσιαστικά, αυτά τα προγράμματα εκτελούνται σε ένα συγκεκριμένο Software και είναι ενεργά στο Διαδίκτυο (Κομνηνός, 2017).

Οποιαδήποτε σύμβαση η οποία συνάπτεται πλέον με ηλεκτρονικά μέσα, ονομάζεται “ηλεκτρονική σύμβαση”.

Οι ηλεκτρονικές συμβάσεις έχουν ειδικές λειτουργίες, επομένως διαφέρουν από τις κλασικές συμβάσεις. Η συμβολή της τεχνολογίας είναι τόσο μεγάλη που οι μέθοδοι που χρησιμοποιούνται και η σύγχρονη τεχνολογία έχουν σημαντικό αντίκτυπο στη νέα μορφή σύμβασης. Στοιχεία όπως οι δηλώσεις προθέσεων και οι τύποι είναι μεταβλητές. Ωστόσο, άλλα στοιχεία, όπως το αντικείμενο της σύμβασης, ο τόπος και ο χρόνος προετοιμασίας και εκτέλεσης της σύμβασης, βασίζονται στα δεδομένα της τεχνολογίας που χρησιμοποιείται. Προκειμένου να καταδειχθεί ο βαθμός διαφοροποίησης των νέων μορφών νομικών πράξεων, εξετάστηκαν βασικά και ασήμαντα στοιχεία. Για τη διεξαγωγή ταυτοποίησης και διερεύνησης, αφενός, είναι απαραίτητο να συγκριθούν οι δύο τύποι παραδοσιακών συμβάσεων και ηλεκτρονικών συμβάσεων, αφενός, για να εκτιμηθεί η χρησιμότητά τους και, αφετέρου, να συγκριθεί η εγκυρότητα και το νομικό καθεστώς των ηλεκτρονικών συμβάσεων. (Κομνηνός, 2017).

Ως εκ τούτου, έχει παρατηρηθεί ότι ενώ τα παραδοσιακά συμβόλαια συντάσσονται σε έντυπη (σε χαρτί) μορφή και περιορισμένα πρωτότυπα αντίγραφα, τα σύγχρονα ή ηλεκτρονικά συμβόλαια συντάσσονται ηλεκτρονικά, έχουν ηλεκτρονικές μορφές και είναι δυνατόν να πραγματοποιούνται συναλλαγές απευθείας ή ταυτόχρονα σε παγκόσμια κλίμακα. (Κομνηνός, 2017).

Ωστόσο, και οι δύο τύποι συμβάσεων ενδέχεται να περιλαμβάνουν δύο ή περισσότερα μέρη. Η προφανής διαφορά μεταξύ των παραδοσιακών συμβάσεων και των ηλεκτρονικών συμβολαίων έγκειται στη μορφή τους, όπως φαίνεται παρακάτω:

- Παραδοσιακή σύμβαση



- Έντυπη μορφή (σε χαρτί)
- Ιδιόχειρη υπογραφή Ηλεκτρονική σύμβαση
- Ψηφιακή μορφή (ηλεκτρονικό έγγραφο)
- Ηλεκτρονική υπογραφή
- Άμεση και γρήγορη αποστολή στα συμβαλλόμενα μέρη

Η σύγχρονη τεχνολογία μπορεί να επιτρέψει τη διατύπωση νομικών ενεργειών με ηλεκτρονικά μέσα. Ωστόσο, ανάλογα με το αντικείμενο, η εκτέλεση της νομικής πράξης μπορεί επίσης να πραγματοποιηθεί μόνο ηλεκτρονικά. (Ιγγλεζάκης, 2008)

Το εύρος των ηλεκτρονικών νομικών ενεργειών συνοψίζεται κυρίως στη χρήση του Διαδικτύου και το γεγονός αυτό προωθεί επίσης τη χρήση ηλεκτρονικών μέσων. Επομένως, η συμβολή του Διαδικτύου στις νομικές ενέργειες επέφερε αλλαγές στο κανονιστικό του πλαίσιο. Διαδικτυακή τεχνολογία επηρεάζει σημαντικά τη σύσταση των εν λόγω δικαιοπραξιών τυπικά και ουσιαστικά. (Ιγγλεζάκης, 2008)

Σε γενικότερο πλαίσιο όμως οι νέες τεχνολογίες δεν θα αλλάξουν την ουσία των κανόνων του εμπορικού δικαίου στον εμπορικό τομέα. Εξαλείφει μόνο τη διαπροσωπική σχέση μεταξύ εμπόρων σε μεγάλο βαθμό και εισάγει τους απρόσωπους παράγοντες της εποχής μας στον εμπορικό νόμο και εισάγει επίσης τη «εκβιομηχάνιση» της πληροφορίας και της επικοινωνίας. (Ιγγλεζάκης, 2008)

Συμβάσεις στο διαδίκτυο

Ένα κοινό χαρακτηριστικό των διαδικτυακών συμβάσεων είναι ότι βασίζονται κυρίως σε προ-συντονισμένα ηλεκτρονικά έγγραφα. Συνδυάζουν συνήθως συμβόλαια και συμβόλαια με τυποποιημένους γενικούς όρους συναλλαγών (ΓΟΣ). (Ιγγλεζάκης, 2008)

Πρόκειται για μεγάλα συμβόλαια με προκαθορισμένους γενικούς εμπορικούς όρους των οποίων ο μελλοντικός αντισυμβαλλόμενος χρήστες Διαδικτύου δεν έχουν άλλη επιλογή από το να επιλέξουν συμφωνία ή να απορρίψουν τη σύμβαση. Οι ΓΟΣ που περιέχονται στον ιστότοπο της υπηρεσίας ή του παρόχου προϊόντων ή στο ηλεκτρονικό ταχυδρομείο που στέλνει στον χρήστη πελάτη πρέπει να γίνει εκ των προτέρων για έναν απροσδιόριστο αριθμό μελλοντικών συμβάσεων. Οι ΓΟΣ δεν είναι δεσμευτικοί ως προς τον καταναλωτή, εάν αγνοεί αδικαιολόγητα τον καταναλωτή κατά την



προετοιμασία της σύμβασης και ο προμηθευτής δεν υποδεικνύει την ύπαρξη του καταναλωτή. (Ιγγλεζάκης, 2008)

Όσον αφορά τις συμβάσεις μεταξύ χρηστών του Διαδικτύου και παρόχων αγαθών και υπηρεσιών, οι χρήστες είναι καταναλωτές. Οι γενικοί όροι ή οι ειδικοί νόμοι για τη σύναψη συμβολαίων στο Διαδίκτυο παρέχουν επαρκή προστασία στους χρήστες του Διαδικτύου που καταναλώνουν υπηρεσίες ή αγαθά μέσω του Διαδικτύου για την υπογραφή συμβάσεων από απόσταση. (Ιγγλεζάκης, 2008)

Μια απομακρυσμένη σύμβαση αναφέρεται σε οποιαδήποτε απομακρυσμένη σύμβαση οργάνωσης για αγαθά ή υπηρεσίες μεταξύ ενός προμηθευτή και ενός καταναλωτή. Η επικοινωνία μεγάλων αποστάσεων αναφέρεται σε οποιοδήποτε μέσο επίτευξης συμβολαίου χωρίς την προσωπική συμμετοχή προμηθευτών και καταναλωτών. (Καράκωστα, 1997)

Για να είναι έγκυρη η σύμβαση πρέπει να περιέχει τα ακόλουθα στοιχεία:

- την ταυτότητα του προμηθευτή,
- τα ουσιώδη χαρακτηριστικά του αγαθού ή της υπηρεσίας,
- την τιμή,
- την ποσότητα και τις δαπάνες μεταφοράς,
- το φόρο προστιθέμενης αξίας, εφόσον δεν περιλαμβάνεται στην τιμή
- τον τρόπο πληρωμής,
- τον τρόπο παράδοσης και εκτέλεσης,
- τη διάρκεια ισχύος της προσφοράς ή της τιμής,
- το κόστος χρησιμοποίησης του μέσου επικοινωνίας από απόσταση και την ελάχιστη διάρκεια ισχύος της σύμβασης.

(Ζέκος, 2017)

Πρέπει επίσης να γνωρίζει την προθεσμία και τους όρους υπαναχώρησης. Το δικαίωμα υπαναχώρησης είναι να δοθεί στους καταναλωτές από τη σύμβαση σε σύντομο χρονικό διάστημα μετά τη σύναψη της σύμβασης. (Ιγγλεζάκης, 2008)

Οι ηλεκτρονικές συμβάσεις στο διαδίκτυο (On line συμβάσεις) λαμβάνουν συνήθως δύο μορφές:



1. είναι οι συνήθειες ηλεκτρονικές συμβάσεις μη τυποποιημένου μηνύματος
2. και οι συμβάσεις Ηλεκτρονικής Ανταλλαγής Δεδομένων – EDI (electronic data interchange), οι οποίες έχουν σαν βάση το τυποποιημένο μήνυμα.

Τι είναι η EDI (electronic data interchange)

Η ζήτηση για πιο άνετη ανταλλαγή δεδομένων στο Διαδίκτυο οδήγησε στην ανάπτυξη μεθόδων τυποποίησης δεδομένων. Η σύμβαση EDI περιέχει τυπικές πληροφορίες, παρέχοντας η Δελούκα-Ιγγλέση, το μεταφράζει στην ελληνική γλώσσα ως ηλεκτρονική ανταλλαγή εμπορικών δεδομένων, η δυνατότητα δηλαδή αυτοματοποίησης της παραγγελίας και της διαδικασίας σύναψης και πληρωμής. (Ιγγλεζάκης, 2008)

Η ηλεκτρονική ανταλλαγή δεδομένων – EDI, είναι μια μέθοδος μετάδοσης πληροφοριών με ηλεκτρονικά μέσα και με την ελάχιστη ανθρώπινη παρέμβαση, μεταξύ συστημάτων πληροφορικής εμπορικών εταιρών, με την ανταλλαγή δεδομένων, τα οποία είναι δομημένα βάσει προτύπων. (Ιγγλεζάκης, 2008)

Χρησιμοποιώντας τυπικά μηνύματα EDI, τα δεδομένα μπορούν να αποστέλλονται με ταχύτατους ρυθμούς, αποτελεσματικά και με ακρίβεια, όσο μεγάλο μέγεθος και αν έχει το εσωτερικό υλικό και λογισμικό του χρήστη και μπορούν να εκτελεστούν διαφορετικά και ασύμβατα συστήματα υπολογιστή. (Ιγγλεζάκης, 2008)

Συμβάσεις EDI

Πρόκειται για συμβάσεις ανταλλαγής δεδομένων μεταξύ προκαθορισμένων μερών και συνήθως λαμβάνουν χώρα σε κλειστά δίκτυα. Το περιεχόμενο των συμβάσεων αυτών είναι περιορισμένο και αφορά στην ανταλλαγή δεδομένων. Ενώ, της σύναψης των συμβάσεων αυτών προηγείται σύμβαση τυποποίησης, στην οποία εμπεριέχονται οι όροι της ηλεκτρονικής επικοινωνίας. (Ιγγλεζάκης, 2008)

Με την EDI υπάρχει η δυνατότητα να είναι επιτυχημένη η ασφαλής, έγκυρη και ταχύτερη μετάδοση των δεδομένων στην ηλεκτρονική μεταφορά συμβάσεων.

- Με τη συμφωνία και των δύο μερών της συναλλαγής, τα δεδομένα μορφοποιούνται σε προκαθορισμένη μορφή τυπικών μηνυμάτων.



- Στο παρελθόν είχε μια τυποποιημένη σύμβαση που περιείχε όρους για ηλεκτρονικές επικοινωνίες.
- Κωδικοποιούνται από τον αποστολέα χρησιμοποιώντας ειδικό λογισμικό υπολογιστή και αποκωδικοποιούνται από τον υπολογιστή του δέκτη.

Υπάρχει πληθώρα από τα πλεονεκτήματα τα οποία προσφέρει η EDI και είναι μέγιστης σημασίας:

- Αυξήθηκε η ταχύτητα της επικοινωνίας, αυξήθηκε η ακρίβεια και τα λάθη δεν υπάρχουν πλέον.
- Μειώνοντας την ποσότητα χαρτιού, τα έξοδα διαχείρισης και το κόστος του προσωπικού (αποδοτικότητα κόστους), με αυτόν τον τρόπο υπάρχει η δυνατότητα να εξοικονομηθούν πολλά χρήματα.
- Εξασφάλιση καλύτερης διαχείρισης και ελέγχου της παραγωγής, παράδοσης, ζήτησης στην αγορά και μειωμένου αποθέματος (καλύτερη εφοδιαστική και αυξημένη παραγωγικότητα).

Επίσης παρουσιάζονται και μειονεκτήματα τα οποία μειώνουν την αξία της χρήσης.

- Το πιο σημαντικό από αυτά είναι η πολυπλοκότητα της χρήσης, η συνήθης πρακτική της επαλήθευσης μηνυμάτων, η μικρή ποσότητα δεδομένων κινητής τηλεφωνίας και η γενική πολυπλοκότητα της επικοινωνίας, που περιορίζουν σε μεγάλο βαθμό τη χρήση αυτής της σύμβασης.
- Επιπλέον, η σύνδεση με το ανοιχτό δίκτυο είναι επίσης πρόβλημα. Σε σύγκριση με το ανοιχτό δίκτυο, το κόστος σύνδεσης είναι υψηλότερο.



ΚΕΦΑΛΑΙΟ 2^ο Η τεχνολογία στο δημόσιο τομέα και ψηφιακή κυβέρνηση

Με την ανάπτυξη της τεχνολογίας, τα τμήματα δημόσιας διοίκησης χρησιμοποιούν το Διαδίκτυο για την παραγωγή και διανομή πληροφοριών, υπηρεσιών και προϊόντων σε πολίτες και επιχειρήσεις, καθιστώντας τους έτσι πιο αποτελεσματικούς και πιο ικανούς να ανταποκριθούν στις σύγχρονες απαιτήσεις. (Ιγγλεζάκης, 2008)

Η «ψηφιακή κυβέρνηση» διασφαλίζει την παροχή υψηλής ποιότητας και ασφαλών ψηφιακών υπηρεσιών του δημόσιου τομέα στους πολίτες, καθώς και την ασφάλεια της χρήσης νέων τεχνολογιών. Όσον αφορά τις υπηρεσίες των πολιτών και την άμεση παροχή εύχρηστων ηλεκτρονικών υπηρεσιών σε όλους τους πολίτες ως κύριο στόχο, τη βελτίωση της αποτελεσματικότητας και της διαφάνειας των συναλλαγών μεταξύ του δημόσιου τομέα και των πολιτών. (Ιγγλεζάκης, 2008)

Η μετεξέλιξη της παραδοσιακής κυβέρνησης σε ψηφιακή περιλαμβάνει τα εξής στάδια:

1. Το πρώτο στάδιο χαρακτηρίζεται από την κυβέρνηση που χρησιμοποιεί διαδικτυακούς τόπους (ιστότοπους) για την παροχή πληροφοριών σε ενδιαφερόμενα άτομα και την απάντηση στις πιο συχνές ερωτήσεις του κοινού.
2. Το δεύτερο στάδιο χαρακτηρίζεται από τις προσπάθειες της χώρας να παρέχει μεγάλο αριθμό συναλλαγών σε ψηφιακή μορφή. Αυτές οι συναλλαγές μπορούν να ολοκληρωθούν ηλεκτρονικά ή σε κάποιο βαθμό με ηλεκτρονικά μέσα και στη συνέχεια να ολοκληρωθούν με παραδοσιακά μέσα.
3. Στο τρίτο στάδιο, η ψηφιακή κυβέρνηση έχει την ευκαιρία να παρέχει άλλες καινοτόμες μεθόδους διαλόγου και συμμετοχής με τους πολίτες, καθώς τα ηλεκτρονικά μέσα διευκολύνουν τους πολίτες να παρακολουθούν την πρόοδό τους, η ψηφιακή κυβέρνηση είναι πιο προσιτή και πιο διαφανής στην πορεία του κυβερνητικού έργου.



Ηλεκτρονική διακυβέρνηση και ηλεκτρονικές συμβάσεις στον δημόσιο τομέα

Η ηλεκτρονική διακυβέρνηση αναφέρεται στην κυβέρνηση που χρησιμοποιεί την τεχνολογία πληροφοριών και επικοινωνιών (ICT-Information and Communication Technology), ειδικά του Διαδίκτυο. Παρέχεται από όλες τις δημόσιες υπηρεσίες και τους κυβερνητικούς αξιωματούχους, ο σκοπός είναι η επεξεργασία και η προώθηση των ηλεκτρονικών συναλλαγών των πολιτών, η βελτίωση της παραγωγικότητας των επιχειρήσεων και των οργανισμών και η καθημερινή ζωή των πολιτών και η επίτευξη βιώσιμης οικονομικής ανάπτυξης. (Ιγγλεζάκης, 2012)

Η ηλεκτρονική διακυβέρνηση μπορεί να αλλάξει ολόκληρο τον δημόσιο τομέα επειδή βοηθά στην καταπολέμηση της γραφειοκρατίας και εξοικονομεί χρόνο για την αντιμετώπιση πολιτών, επιχειρήσεων, οργανισμών και εταιρικών υποθέσεων στη δημόσια διοίκηση. Μπορεί επίσης να συμβάλει στη μείωση του λειτουργικού κόστους των υπηρεσιών του δημόσιου τομέα και ταυτόχρονα να μειώσει τις αδυναμίες των διοικητικών δράσεων που δεν επέτρεψαν ακόμη στις δημόσιες υπηρεσίες να ανταποκριθούν στις τρέχουσες προκλήσεις και τις αναπτυξιακές ανάγκες της χώρας. (Ιγγλεζάκης, 2012)

Προκειμένου να εφαρμοστεί η ηλεκτρονική διακυβέρνηση και να επωφεληθούν τα περισσότερα οφέλη από την εφαρμογή, είναι απαραίτητο να βρεθούν και να εξοικονομηθούν απαραίτητοι οικονομικοί πόροι, να χρησιμοποιηθεί η κατάλληλη τεχνολογία και η μεταφορά τεχνογνωσίας, κυρίως όμως είναι η αλλαγή στην νοοτροπία τόσο των δημόσιων λειτουργών, όσο και των πολιτών και των επιχειρήσεων. (Ιγγλεζάκης, 2012)

Η ηλεκτρονική διακυβέρνηση έχει ποικίλα πλεονεκτήματα και είναι και εξίσου μεγίστης σημασίας. Πρώτον, η υιοθέτηση ηλεκτρονικών υπηρεσιών μπορεί να διασφαλίσει ότι το λειτουργικό κόστος των δημοσίων υπηρεσιών μειώνεται, καθώς μεγάλο μέρος των συναλλαγών έχουν μετατραπεί από παραδοσιακές υπηρεσίες σε ηλεκτρονικές υπηρεσίες. Δεδομένου ότι η υπηρεσία μπορεί να ολοκληρωθεί από μικρότερο αριθμό υπαλλήλων, απλοποιεί και επιταχύνει τις διοικητικές διαδικασίες, μειώνει το κόστος αγοράς χαρτιού, έντυπων εντύπων, εγγράφων αλληλογραφίας και κόστους προσωπικού. Δεύτερον, να παρέχουν στους πολίτες καλύτερες υπηρεσίες, διότι οι δημόσιες υπηρεσίες μπορούν να ανταποκρίνονται στις απαιτήσεις τους άμεσα



και αποτελεσματικά, γεγονός που μειώνει σημαντικά το γραφειοκρατικό φόρτο τους και εξοικονομεί πολύ χρόνο αναμονής, αλλά παρέχει κυρίως τη δυνατότητα παντός καιρού υπηρεσίες. Τρίτον, παρέχοντας στους πολίτες ισότιμη πρόσβαση σε νέες τεχνολογίες επεκτείνοντας περαιτέρω τις ευρυζωνικές υποδομές και υπηρεσίες, και τελικά πραγματοποιώντας την αναδιοργάνωση των δημόσιων υπηρεσιών, βελτίωσαν την αποτελεσματικότητά τους και τις συνολικές δυνατότητες διοικητικής διαχείρισης των υπηρεσιών δημόσιας διοίκησης. (Ιγγλεζάκης, 2012)

Είναι προφανές ότι τα οφέλη της ηλεκτρονικής διακυβέρνησης είναι τόσο ισχυρά που αποδεικνύει πλήρως ότι κάθε επιχείρηση ηλεκτρονικής διακυβέρνησης υπηρεσιών δημόσιου τομέα απαιτεί πολύ χρόνο, χρήμα και επενδύσεις στην ανάπτυξη ανθρώπινου δυναμικού. Πάντα δεσμευμένος για τη βελτίωση της ποιότητας ζωής των πολιτών, την αύξηση της παραγωγικότητας και την επιτάχυνση της οικονομικής ανάπτυξης των σύγχρονων χωρών. (Ιγγλεζάκης, 2012)

Επιθεωρώντας τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, διαπιστώσαμε ότι διαφέρουν στα προγράμματα υπηρεσιών ηλεκτρονικής διακυβέρνησης πολιτών (GOvernment - to - Citizen (G2C) services) ή επιχειρήσεων (GOvernment - to - Business (G2B) Services) και άλλων δημόσιων υπηρεσιών (GOvernment - to - GOvernment (G2C) services), Προκειμένου να απλοποιηθεί η σχέση μεταξύ διαχείρισης και παραληπτών υπηρεσιών, βασίζεται σε μια μέθοδο εκτίμησης του βαθμού ολοκλήρωσης μιας υπηρεσίας μεμονωμένης τοποθεσίας, που τα σχήματα ηλεκτρονικής εξυπηρέτησης διακρίνονται σε σχήματα πρώτης επαφής, σχήματα ποικιλίας συναλλαγών, σχήματα πρώτης στάσης και σχήματα μοναδικής στάσης. (Ιγγλεζάκης, 2012)

Στη συνέχεια, το σχέδιο ηλεκτρονικής υπηρεσίας χωρίζεται στο σχέδιο που σχετίζεται με την πληροφόρηση, την επικοινωνία, τη συναλλαγή και τη διανομή υπηρεσιών, και τέλος διαιρείται στο σχέδιο ηλεκτρονικής υπηρεσίας που αναφέρεται στα τέσσερα στάδια (4- stage framewOrk). Η Ευρωπαϊκή Ηλεκτρονική Πρωτοβουλία τις χρησιμοποιεί για να αξιολογήσει την πρόοδο των υπηρεσιών ηλεκτρονικής διακυβέρνησης στα κράτη μέλη και, σύμφωνα με την πρόοδο, την ολοκλήρωση των υπηρεσιών ηλεκτρονικής διακυβέρνησης διαχωρίζεται από τα στάδια της απλής



πληροφόρησης, της μονόδρομης επικοινωνίας, της αμφίδρομης επικοινωνίας και της πλήρους εξυπηρέτησης συναλλαγών. (Ιγγλεζάκης, 2012)

Στην πρώτη φάση, η εκτεταμένη εφαρμογή της ηλεκτρονικής διακυβέρνησης θα μειώσει τις κρατικές δαπάνες κατά 10% σε 25%. Ταυτόχρονα, αυτό θα μειώσει τη γραφειοκρατία και τη διαφθορά, διότι σε γενικές γραμμές, οι πολίτες και οι δημόσιες διοικήσεις σε σπάνιες περιπτώσεις θα επικοινωνήσουν άμεσα με κυβερνητικούς αξιωματούχους, επειδή θα «συναλλαγή» μέσω του Διαδικτύου, χάρη στην τηλεματική λειτουργία του μηχανισμού. (Ιγγλεζάκης, 2012)

Στη σύγχρονη ευρωπαϊκή κοινωνία, οι οικονομικοί και πολιτικοί εμπλέκονται καθημερινά, κυρίως μέσω της κατανομής δημοσίων έργων και δημοσίων συμβάσεων σε ιδιώτες επιχειρηματίες. Η Ευρωπαϊκή Ένωση έχει καταβάλει σοβαρές προσπάθειες για τη μείωση της διαφθοράς σε όλα τα κράτη μέλη της σε αυτόν τον τομέα. Από την πλευρά τους, τα κράτη μέλη έχουν θεσπίσει κανόνες σε αυτόν τον τομέα, ιδίως ενοποιώντας τη νομοθεσία τους για να διασφαλίσουν τον τελικό στόχο του θεμιτού ανταγωνισμού. (Ιγγλεζάκης, 2012)

Το εθνικό δίκτυο δημόσιας διοίκησης ΣΥΖΕΥΞΙΣ

Το "Εθνικό Δίκτυο Δημόσιας Διοίκησης ΣΥΖΕΥΞΙΣ" είναι ένα έργο του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης (ΥΠΕΣΔΔΑ), το οποίο άρχισε να λειτουργεί τον Δεκέμβριο του 2005 και στοχεύει στην ανάπτυξη και τον εκσυγχρονισμό των δημόσιων τηλεπικοινωνιακών υποδομών. Είναι το δίκτυο πρόσβασης και το δίκτυο κορμού των δημόσιων ιδρυμάτων που καλύπτουν όλες τις ανάγκες επικοινωνίας μεταξύ τους μέσω τηλεφώνου (τηλεφωνική επικοινωνία μεταξύ ιδρυμάτων), δεδομένων (επικοινωνία μέσω υπολογιστή-Διαδίκτυο) και βίντεο (τηλεδιάσκεψη-τηλεκπαίδευση).

Ο σκοπός του έργου είναι να βελτιώσει τη λειτουργία των δημόσιων υπηρεσιών παρέχοντας προηγμένες υπηρεσίες τηλεματικής και ολοκληρωμένες υπηρεσίες για πολίτες με χαμηλό κόστος, μέσω αυτοματοποιημένων και φιλικών προς τον χρήστη συστημάτων επεξεργασίας πληροφοριών και συναλλαγών, και βελτιώνοντας το επίπεδο επικοινωνίας των δημόσιων υπηρεσιών.



Επίσης το 2007, ολοκληρώθηκε με επιτυχία η σύνδεση μεταξύ ΣΥΖΕΥΞΙΣ και πανευρωπαϊκού δικτύου s-TESTA. Το S-TESTA (Ασφαλής Διευρωπαϊκή Υπηρεσία Τηλεματικής Μεταξύ Διοικήσεων) είναι το πανευρωπαϊκό ιδιωτικό δίκτυο IP της Ε.Ε. Ανεξάρτητα από το Διαδίκτυο, μπορεί να παρέχει ασφαλείς και αξιόπιστες διευρωπαϊκές επικοινωνίες στους οργανισμούς δημόσιας διοίκησης των κρατών μελών της ΕΕ. Το δίκτυο παρέχει υπηρεσίες μόνο στις δημόσιες διοικήσεις των κρατών μελών της ΕΕ. Ιδιαίτερη έμφαση δίνεται στην ασφάλεια και την κρυπτογράφηση των πληροφοριών και στις παραμέτρους ποιότητας (διαθεσιμότητα-απόκριση) των υπηρεσιών δικτύου (SLA) και του εθνικού δικτύου ΣΥΖΕΥΞΙΣ.

Η Διαδικτυακή Πύλη ermis.gov.gr και οι υπηρεσίες της στους πολίτες

Οι διαδικτυακές πύλες (portals) της κυβέρνησης

Οι παραδοσιακοί ιστότοποι διαφόρων υπουργείων παρέχουν συνήθως πληροφορίες με τη μορφή λιστών / μενού που σχετίζονται με την οργανωτική δομή. Πρόκειται για διαδικτυακές εφαρμογές που παρέχουν συνδέσμους προς σχετικούς ιστότοπους και δεν μπορούν να ικανοποιήσουν τις ανάγκες των διαχειριστών επειδή παρέχουν μόνο διαδικτυακή κατάσταση. Οι κυβερνητικές πύλες καλύπτουν αυτό το κενό, επιτρέποντας στους πολίτες / επιχειρήσεις να έχουν εύκολη πρόσβαση στις πληροφορίες και τις υπηρεσίες που παρέχονται από διάφορα υπουργεία. Οι κυβερνητικές πύλες οργανώνονται σύμφωνα με γεγονότα ζωής (όπως γέννηση, γάμος και επιχειρηματικότητα) και παρέχουν πληροφορίες και διαδικτυακές υπηρεσίες για κάθε περίπτωση. Η κυβερνητική πύλη κατασκευάζεται βάσει της ροής των γεγονότων του κύκλου ζωής και εστιάζει στις απαιτήσεις των πολιτών και όχι στις γενικές υπηρεσίες κάθε τμήματος.

Μέσω του συστήματος ανταλλαγής πληροφοριών, οι βάσεις δεδομένων διαφόρων υπουργείων μπορούν να διασυνδεθούν και υπηρεσίες μπορούν να συλλεχθούν και να παρουσιαστούν στους πολίτες ως γεγονότα ζωής. Η ενσωματωμένη κυβερνητική πύλη είναι ένα εργαλείο για την παροχή καλύτερων και περισσότερων κυβερνητικών υπηρεσιών και πληροφοριών προσανατολισμένων προς τους πολίτες. Η διαδικτυακή πύλη κυβερνητικών υπηρεσιών στοχεύει να παρέχει άμεση πρόσβαση σε εφαρμογές, σχετικούς νόμους και κανονισμούς, κυβερνητικά προγράμματα και σε αυτούς που είναι



υπεύθυνοι για αυτές. Σκοπός τους είναι να ξεπεράσουν την πολυπλοκότητα της διαδικασίας απόκτησης κυβερνητικών υπηρεσιών, επειδή όλα στη ζωή αποκτούν πλήρη ηλεκτρονικά στοιχεία από όλους τους συμμετέχοντες δημόσιους οργανισμούς και τη δυνατότητα ηλεκτρονικών συναλλαγών μαζί τους.

Οι πολίτες δεν χρειάζεται να γνωρίζουν ποιο τμήμα / γραφείο χειρίζεται την αίτησή τους και τον περίπλοκο καταμερισμό ευθυνών μεταξύ τους για την απόκτηση υπηρεσιών. Οι πολίτες χρησιμοποιούν κυβερνητικές πύλες επειδή παρέχουν λειτουργικά πλεονεκτήματα, γιατί δεν χρειάζεται να επιλέξουν μέσω λιστών εργασίας, αλλά μέσω λιστών υπηρεσιών. Επιπλέον, οι πολίτες μπορούν επίσης να έχουν ελεύθερη πρόσβαση στα πολλά δημόσια ιδρύματα που εμπλέκονται σωματικά και ηλεκτρονικά. Αντ' αυτού, πραγματοποιούν ηλεκτρονικές συναλλαγές σε "υπηρεσία μίας στάσης" σε συγκεκριμένες εκδηλώσεις ζωής, σαν να υπάρχει μόνο ένας οργανισμός που φέρει όλες τις σχετικές ευθύνες.

Με αυτόν τον τρόπο, οι ΤΠΕ καθιστούν την οργάνωση διεπαφής μεταξύ πολιτών και επιχειρήσεων και της δημόσιας διοίκησης ανεξάρτητη από τους εσωτερικούς τους οργανισμούς και τον καταμερισμό ευθυνών μεταξύ διαφόρων δημόσιων οργανισμών. Τώρα, η διεπαφή οργανώνεται σύμφωνα με τις ανάγκες των διαχειριστών, ενώ οι εσωτερικές λειτουργίες και ευθύνες του τμήματος δημόσιας διοίκησης οργανώνονται σύμφωνα με άλλους στόχους (όπως ελαχιστοποίηση του κόστους).

Υπηρεσίες της Κυβερνητικής Διαδικτυακής Πύλης EPMHΣ

Η πύλη EPMHΣ είναι μια ενοποιημένη κυβερνητική πύλη για τη δημόσια διαχείριση, η οποία μπορεί να παρέχει στους πολίτες και τις επιχειρήσεις πληροφορίες και να παρέχει ασφαλείς υπηρεσίες ηλεκτρονικής διακυβέρνησης. Είναι η «έρευνα και ανάπτυξη της πύλης της κεντρικής κυβέρνησης για τη δημόσια διαχείριση για την επεξεργασία πληροφοριών και ασφάλειας πολιτών / εταιρικών ηλεκτρονικών συναλλαγών» που πραγματοποιείται με τους φορείς υλοποίησης της κοινωνίας της πληροφορίας. Ο οργανισμός λειτουργίας και χρηματοδότησης είναι το Υπουργείο Εσωτερικών-Γενική Γραμματεία Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης. Στο πλαίσιο του εκσυγχρονισμού της δημόσιας διαχείρισης, ο κύριος σκοπός της διαδικτυακής πύλης EPMHΣ είναι να παρέχει στους πολίτες υπηρεσίες προστιθέμενης αξίας. Είναι το κέντρο παροχής ολοκληρωμένων πληροφοριών στους



πολίτες και τις επιχειρήσεις, σχετικά με τις φυσικές και ηλεκτρονικές συναλλαγές με τις δημόσιες διοικήσεις.

Ταυτόχρονα, παρέχει επιλεγμένες υπηρεσίες ηλεκτρονικών συναλλαγών μέσω των οποίων οι πολίτες μπορούν να αποκτήσουν υπηρεσίες εξ ολοκλήρου ηλεκτρονικά. Από επιχειρηματική άποψη, η πύλη EPMHΣ είναι το "ηλεκτρονικό πολυκατάστημα" της δημόσιας διοίκησης, παρέχοντας υπηρεσία μίας στάσης (μονοαπευθυντικό κατάστημα) και κινείται σε 96 κατευθύνσεις με τους ακόλουθους τρεις βασικούς άξονες: Η παροχή πληροφοριών παρέχει συναλλαγές πολιτών Όλες οι πληροφορίες χρειάζονται. Και εταιρείες που παρέχουν όλες τις υπηρεσίες της δημόσιας διοίκησης για τη λήψη αξιόπιστων πληροφοριών. Αυτές οι πληροφορίες γνωστοποιούνται στο κοινό με διαφορετικούς τρόπους.

Σύμφωνα με τα γεγονότα της ζωής (ταξιδεύω, παντρεύομαι, συμμετέχω στο στρατό κ.λπ.), ανάλογα με θέματα (όπως εργασία, ασφάλιση και συντάξεις), αυτά τα θέματα χωρίζονται σε αντίστοιχες υποκατηγορίες (επάγγελμα, κοινωνική ασφάλιση κ.λπ.), ανάλογα με τον χρήστη (όπως ιδιωτικοί υπάλληλοι, Χειροτεχνίες) και δημόσια ιδρύματα, έτσι ώστε οι χρήστες να έχουν πρόσβαση στις πληροφορίες και στα στοιχεία επικοινωνίας των ιδρυμάτων της επιλογής τους. Παροχή δια λειτουργικότητας: Η πύλη EPMHΣ παρέχει την απαραίτητη υποδομή για την πλήρη υποστήριξη της δια λειτουργικότητας μεταξύ δημόσιων συστημάτων πληροφοριών διαχείρισης και παροχής υπηρεσιών ηλεκτρονικών συναλλαγών από κεντρική προοπτική.

Οι χρήστες που είναι εγγεγραμμένοι στην πύλη μπορούν να επωφεληθούν από μεγάλο αριθμό διαδικτυακών υπηρεσιών και να έχουν την ευκαιρία να λάβουν πιστοποιητικά στα εισερχόμενά τους. Ασφάλεια συναλλαγών Η πύλη EPMHΣ χρησιμοποιεί επεκτάσιμες μεθόδους επαλήθευσης ψηφιακής ταυτότητας για την παροχή ασφαλών υπηρεσιών ηλεκτρονικής διακυβέρνησης σε κάθε επίπεδο. Ανάλογα με τον τύπο των δεδομένων που διαβιβάζονται, το EPMHΣ υποστηρίζει διαφορετικά επίπεδα αναγνώρισης. Συγκεκριμένα, για απλές υπηρεσίες πληροφοριών, δεν υπάρχει ανάγκη αναγνώρισης ταυτότητας, ενώ για ηλεκτρονικές υπηρεσίες, πρέπει απλώς να εγγραφείτε χρήστες στο TAXISnet ή να χρησιμοποιήσετε τους κωδικούς τους. Για υπηρεσίες που παρέχουν πλήρη ηλεκτρονική επεξεργασία, εκτός από την εγγραφή, απαιτείται φυσική ταυτοποίηση σε οποιοδήποτε Κ.Ε.Π.



Σήμερα, η κυβερνητική πύλη ΕΡΜΗΣ παρέχει 15 πλήρως αυτοματοποιημένες υπηρεσίες και περίπου 100 μερικώς αυτοματοποιημένες υπηρεσίες. Για να ολοκληρωθεί αυτή η υπηρεσία, οι πολίτες πρέπει να συμμετάσχουν στο ΚΕΠ. Επιπλέον, η κυβερνητική πύλη ΕΡΜΗΣ παρέχει ένα πεδίο "Αναζήτηση" στην αρχική του σελίδα για να βοηθήσει στην εύρεση των πληροφοριών ή της διαδικασίας που αναζητούν οι χρήστες εισάγοντας λέξεις-κλειδιά. Εκτός από τις πληροφορίες που παρέχονται στους χρήστες, μπορείτε επίσης να πραγματοποιήσετε αναζήτηση από το πεδίο "Αναζήτηση", επιλέξτε τα αποτελέσματα που του ενδιαφέρει, παρέχετε επίσης μια λίστα σχετικών υπηρεσιών, ανακοινώσεων και πληροφοριών σχετικά με τις υπηρεσίες που έχει επιλέξει. Επιπλέον, η κυβερνητική πύλη ΕΡΜΗΣ διαθέτει μια λίστα με τις "Συχνές ερωτήσεις" χρήστη για να διευκρινίσει ζητήματα που σχετίζονται με τη χρήση της πύλης. Εάν το πρόβλημά του χρήστη δεν καλύπτεται από τη λίστα "Συχνές ερωτήσεις", μπορείτε να χρησιμοποιήσετε το πεδίο "Επικοινωνία" για να αναφέρετε τυχόν προβλήματα, παραλείψεις και σφάλματα που εντοπίζει.

Τέλος, η πύλη σας επιτρέπει να επιλέξετε πληροφορίες εμφάνισης σε τέσσερις γλώσσες (ελληνικά, αγγλικά, γαλλικά και γερμανικά) και παρέχει μια πλήρη λίστα ιστοτόπων άλλων ιδρυμάτων (όπως εθνικά ποινικά αρχεία).

Ανοίγμα Ηλεκτρονικής Θυρίδας

Η διεύθυνση ηλεκτρονικού ταχυδρομείου που διατίθεται στους αναγνωρισμένους χρήστες της κυβερνητικής πύλης ΕΡΜΗΣ μπορεί να αποθηκεύσει τα απαραίτητα έγγραφα για να χειριστεί τις υποθέσεις τους στη δημόσια διοίκηση. Είναι ένας προσωπικός χώρος αποθήκευσης για ηλεκτρονικά έγγραφα των χρηστών, οι οποίοι μπορούν να ληφθούν με τρεις διαφορετικούς τρόπους:

- α) Ο χρήστης που μπορεί να ανεβάσει το επιλεγμένο έγγραφο στα εισερχόμενά του.
- β) Το Κ.Ε.Π. πραγματοποιεί συγκεκριμένες συναλλαγές ή ψηφιοποιεί έγγραφα από το προσωπικό κατόπιν αιτήματος των χρηστών,
- γ) Μπορεί να λάβει το πιστοποιητικό online από την πύλη ΕΡΜΗΣ, υπό την προϋπόθεση ότι η ηλεκτρονική συναλλαγή υποβάλλεται σε επεξεργασία εξ ολοκλήρου ηλεκτρονικά.



Απλώς συνδέστε τον χρήστη στην πύλη EPMHS για να ολοκληρώσετε την απόκτηση της διεύθυνσης ηλεκτρονικού ταχυδρομείου. Η σύνδεση μεταξύ του χρήστη και της πύλης μπορεί να ολοκληρωθεί με τρεις τρόπους. Χρησιμοποιώντας τον κωδικό που αποκτήθηκε από το TAXISnet, αποκτώντας τον κωδικό από την πύλη EPMHS και χρησιμοποιώντας τον κωδικό eIDAS.

Η ύπαρξη του κουτιού διευκολύνει την εφαρμογή ηλεκτρονικών υπηρεσιών που απαιτούν ενδιάμεσα έγγραφα μέσω της πύλης EPMHS, όπως αντίγραφα πιστοποιητικών γέννησης, αστυνομικές ταυτότητες, στρατιωτικά πιστοποιητικά ταυτότητας κ.λπ. Μαζί με αιτήσεις σε ενδιαφερόμενα ιδρύματα. Για τους απλούς χρήστες της πύλης EPMHS, τα έγγραφα φυλάσσονται στο γραμματοκιβώτιο για τρεις ημέρες. Εάν ο χρήστης περάσει το Κ.Ε.Ρ. τότε το αρχείο θα διατηρηθεί στο γραμματοκιβώτιο για έξι μήνες. Προκειμένου να κάνει απεριόριστη απώλεια αρχείων στο πλαίσιο e-mail, ο χρήστης θα πρέπει να εκδώσει ένα προσωπικό ψηφιακό πιστοποιητικό.

Το ηλεκτρονικό ταχυδρομείο είναι ένα ασφαλές μέρος. Τα άτομα που χρειάζονται έγγραφα μπορούν να πάνε εκεί για να βρουν έγγραφα μετά την ηλεκτρονική εξουσιοδότηση του χρήστη. Το χρηματοκιβώτιο παρέχει όλους τους μηχανισμούς ασφαλείας, έτσι ο αντίστοιχος χειριστής μπορεί να χρησιμοποιήσει μεθόδους κρυπτογράφησης / αποκρυπτογράφησης για πρόσβαση μόνο στα έγγραφα που απαιτούνται από τον χρήστη. Επιπλέον, οι φυσικώς επικυρωμένοι χρήστες μπορούν να λάβουν τα έγγραφά τους και να τα αποθηκεύσουν στα ηλεκτρονικά κουτιά τους για μελλοντική χρήση μέσω οποιασδήποτε ζητούμενης υπηρεσίας.

Αρχή πιστοποίησης του ελληνικού δημοσίου

Το Υπουργείο Εξωτερικών έχει διαμορφώσει ένα οργανωτικό και θεσμικό πλαίσιο, καθώς και τους απαραίτητους διοικητικούς μηχανισμούς. Επομένως, από τη μία πλευρά, οι σχετικές διαδικασίες είναι απολύτως νόμιμες και, αφετέρου, μπορεί να καλύψει τις ανάγκες όλων των δημόσιων υπηρεσιών. Σχετικές ερωτήσεις. Η υποδομή δημόσιου κλειδιού που έχει δημιουργηθεί βασίζεται σε μια ιεραρχία ευθυνών. Συγκεκριμένα, η οργανωτική δομή του διοικητικού μηχανισμού που δημιούργησε το



Υπουργείο Εξωτερικών για την υποστήριξη της λειτουργίας υποδομών δημόσιου κλειδιού έχει ως εξής:

1. Σύμφωνα με άρθρο του νόμου 910/2014 το «Ελληνικό Εθνικό Κέντρο Πιστοποίησης» (ΑΠΕΔ) ορίζεται ως «Κέντρο Πιστοποίησης Κεφαλαίου» (ΚΠΚ), Υπουργείο Εξωτερικών Υπηρεσία Ανάπτυξης Πληροφορικής της Γενικής Γραμματείας Δημόσιας Διοίκησης και Ηλεκτρονικής Διακυβέρνησης.

Η ΑΠΕΔ είναι υπεύθυνη για την «έκδοση ψηφιακών πιστοποιητικών για άλλες δημόσιες υπηρεσίες ή ιδρύματα του δημόσιου τομέα για την πιστοποίηση της πιστοποίησης, του προσδιορισμού κατεύθυνσης και του συντονισμού των υπηρεσιών που παρέχονται από τον δημόσιο τομέα» (άρθρο του νόμου 910/2014).

2. Η «Βασική Αρχή Πιστοποίησης» (ΥΠΑΠ) του Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης ορίζεται ως τμήμα επεξεργασίας και μόνιμου αποθέματος του Σχεδίου Υπηρεσιών Ανάπτυξης Πληροφορικής και Γραφείου Εφαρμογών της Γενικής Διοίκησης Δημόσιας και Ανάπτυξης.

Η ΥΠΑΠ είναι υπεύθυνη για την έκδοση και τη γενική διαχείριση πιστοποιητικών τελικού χρήστη, καθώς και για την εποπτεία και τον έλεγχο της ορθής και νόμιμης λειτουργίας των υπηρεσιών PKI.

3. Η «Αρχή Εγγραφής» (ΑΕ) του Υπουργείου Εξωτερικών ορίζεται ως τμήμα υλοποίησης και λειτουργίας του έργου και του συστήματος «Κοινωνίας της Πληροφορίας ΑΕ – ΚτΠ Α.Ε.».

Το καθήκον του οργανισμού εγγραφής είναι να υποστηρίζει τις υπηρεσίες πιστοποίησης που παρέχονται στους σχετικούς κανονισμούς πιστοποίησης (ΚΠ). Συγκεκριμένα, η αρχή εγγραφής είναι υπεύθυνη για τον εντοπισμό, την αποδοχή ή την απόρριψη ηλεκτρονικών καταχωρίσεων για την έκδοση πιστοποιητικών και για την αποδοχή ή απόρριψη αιτημάτων ακύρωσης, ανάκτησης ή ανανέωσης πιστοποιητικών βίζας.

4. Ως «**Εντεταλμένα Γραφεία**» (ΕΓ), ορίζονται τα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ), σε ολόκληρη τη χώρα.



Σύμφωνα με κανονισμούς, το εξουσιοδοτημένο γραφείο είναι κυρίως υπεύθυνο για την επεξεργασία και ενέργειες που σχετίζονται με την ταυτοποίηση δεδομένων και τις εφαρμογές τελικών χρηστών (όπως δημόσιοι υπάλληλοι), οι οποίες σχετίζονται με ψηφιακές υπογραφές και πιστοποιητικά κρυπτογράφησης στο σχετικό ΚΠ.

Σε συνεργασία με την ΚτΠ Α.Ε., η ΥΠ.ΕΣ.Δ.Δ.Α. έχει αναπτύξει μια κατάλληλη υποδομή που μπορεί να υποστηρίξει αντίστοιχους μηχανισμούς διαχείρισης που μπορούν να δημιουργήσουν άλλες κυβερνητικές υπηρεσίες. Αυτό που πρέπει να διευκρινιστεί είναι ότι προτού σχηματίσουν άλλοι φορείς αντίστοιχοι μηχανισμοί, σύμφωνα με το άρθρο 20 του ν. 4727/2020 μπορούν να παρέχονται διοικητικοί μηχανισμοί και υπηρεσίες υποδομής.

Επιπλέον, έχει εγκριθεί από την ΕΕΤΤ(Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων) και έχει εγκριθεί από το Υπουργείο Εσωτερικών, το Υπουργείο Δημόσιας Διοίκησης και Αποκέντρωσης και Μεταφορών και Επικοινωνιών, και έχει εγκριθεί από την JMC ο "Κανονισμός Πιστοποίησης-ΑΠΕΔ", ο οποίος ορίζει τους όρους και τις προϋποθέσεις των υπηρεσιών πιστοποίησης που παρέχονται από τα ακόλουθα τμήματα: ΑΠΕΔ. Ο σχετικός κανονισμός είναι η Δήλωση Πρακτικής ΑΠΕΔ, η οποία χρησιμοποιείται για την παροχή υπηρεσιών πιστοποίησης σύμφωνα με τον νόμο 4727/2020 για Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις για την έκδοση «αναγνωρισμένων πιστοποιητικών».

Η προϋπόθεση των ασφαλών υπηρεσιών επικοινωνίας και ηλεκτρονικών συναλλαγών είναι ότι ο τελικός χρήστης του σχετικού ιδρύματος (το φυσικό πρόσωπο που εκδίδει ψηφιακό πιστοποιητικό κατόπιν αιτήματος) έχει δύο ψηφιακά πιστοποιητικά, ένα για ψηφιακή υπογραφή και ένα για κρυπτογράφηση. Το ψηφιακό πιστοποιητικό (και το σχετικό ζεύγος κλειδιών) δημιουργείται από μια συσκευή ασφαλείας, εκδίδεται ηλεκτρονικά από το Υπουργείο Εσωτερικών και αποθηκεύεται με ασφάλεια σε μια συσκευή υπογραφής ασφαλείας που μπορεί να χρησιμοποιηθεί από τον τελικό χρήστη, όπως μια έξυπνη κάρτα ή ένα διακριτικό usb. Στην πρώτη φάση της υπηρεσίας



PKI(public key infrastructure), παρέχονται επίσης οι απαραίτητες συσκευές ανάγνωσης καρτών.

Τα ψηφιακά πιστοποιητικά είναι αυστηρά προσωπικά πιστοποιητικά και χρησιμοποιούνται μόνο για την εκτέλεση των καθηκόντων των κατόχων τους για την κάλυψη των αναγκών εξυπηρέτησης των ιδρυμάτων τους. Οι ενδεικτικές χρήσεις ψηφιακών πιστοποιητικών είναι:

- Ασφαλής παράδοση email / μηνυμάτων (υπογραφή και κρυπτογράφηση)
- Υπογραφή και κρυπτογράφηση ηλεκτρονικών εγγράφων (όπως έγγραφα Adobe Acrobat, έγγραφα Word)
- Ασφαλής ηλεκτρονική αναγνώριση
- Έλεγχος της πρόσβασης σε κατάλληλες εφαρμογές.

Σύμφωνα με τους "Κανόνες πιστοποίησης", οι όροι (και οι υποχρεώσεις) για την έκδοση ψηφιακών πιστοποιητικών σε τελικούς χρήστες περιλαμβάνουν:

- Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται μόνο για εγκεκριμένους και νομικούς σκοπούς σύμφωνα με τους κανονισμούς πιστοποίησης.
- Οι τελικοί χρήστες πρέπει να λαμβάνουν υπόψη τους περιορισμούς στη διαχείριση πιστοποιητικών και τη χρήση που αναφέρονται στους κανονισμούς πιστοποίησης.
- Η έξυπνη κάρτα (ή το διακριτικό USB) και ο αντίστοιχος κωδικός PIN-PUK είναι αυστηρά προσωπικοί και ο τελικός χρήστης είναι πλήρως υπεύθυνος για τη χρήση και την ασφαλή αποθήκευσή του. Ο τελικός χρήστης δεν πρέπει να εκθέτει την έξυπνη κάρτα οπουδήποτε, ακόμη και στο χώρο εργασίας.
- Ο τελικός χρήστης θα πρέπει να υπογράψει την έξυπνη κάρτα στο ειδικό πλαίσιο στο πίσω μέρος.
- Ο τελικός χρήστης δεν πρέπει να δανείζει την έξυπνη κάρτα ή να αποκαλύπτει τον κωδικό PIN-PUK σε κανέναν.



- Εάν υπάρχουν προβλήματα ή δημιουργηθεί κάποια συμπεριφορά που παραβιάζει τους παραπάνω κανονισμούς ή εάν η έξυπνη κάρτα χαθεί, κλαπεί ή καταστραφεί, ο τελικός χρήστης πρέπει να ενημερώσει αμέσως τον οργανισμό εγγραφής στον οποίο ανήκει.
- Εάν τερματιστεί η σχέση εργασίας με το γραφείο εργασίας, ο τελικός χρήστης πρέπει να ενημερώσει το πρακτορείο εγγραφής και η έξυπνη κάρτα θα ανακληθεί και θα επιστραφεί στο πρακτορείο.
- Ο τελικός χρήστης αποδέχεται όλα τα δικαιώματα και τις υποχρεώσεις που απορρέουν από τους κανονισμούς πιστοποίησης ΑΠΕΔ (Αρχή Πιστοποίησης Ελληνικού Δημοσίου) υποβάλλοντας αίτηση για απόκτηση ψηφιακού πιστοποιητικού.

Τα φυσικά πρόσωπα που βασίζονται στα δεδομένα που περιέχονται σε ψηφιακά πιστοποιητικά που εκδίδονται σύμφωνα με τις διατάξεις του ΚΠ, ονομάζονται Τρίτος Συμμετέχων (ΤΣ).

- Ο Τρίτος Συμμετέχων πρέπει να έχει πρόσβαση σε επαρκείς πληροφορίες που του παρέχονται από την υποδομή δημόσιου κλειδιού ΑΠΕΔ και τους ιστότοπους που αναφέρονται σε αυτήν την εγκύκλιο μέσω του Διαδικτύου για να του επιτρέψει να ελέγξει αν βασίζεται σε ψηφιακά πιστοποιητικά.
- Οι συμμετέχοντες τρίτων πρέπει να έχουν σύγχρονες και κατάλληλες εφαρμογές (όπως προγράμματα περιήγησης Διαδικτύου, copywriters, κ.λπ.) για να "λάβουν αυτόματα" όλα τα απαραίτητα μέτρα για να ελέγξουν την εγκυρότητα των πιστοποιητικών που παρέχονται στους "Κανονισμούς πιστοποιητικών".
- Ο Τρίτος Συμμετέχων θα πρέπει να λάβει υπόψη τους περιορισμούς χρήσης του πιστοποιητικού (υπογραφή ή κρυπτογράφηση) που αναφέρονται στους "Κανόνες πιστοποίησης ΑΠΕΔ".

Οφέλη

Ο κύριος σκοπός είναι να βελτιωθεί η λειτουργία της ελληνικής δημόσιας διοίκησης βελτιώνοντας την ποιότητα των τηλεπικοινωνιακών υπηρεσιών και παρέχοντας προηγμένες τηλεματικές υπηρεσίες. Οι επιδιωκόμενοι στόχοι είναι:



- Πραγματοποιήστε τον εκσυγχρονισμό της δημόσιας διοίκησης στην Ελλάδα (η υλοποίηση του μοντέλου ηλεκτρονικής κυβέρνησης) παρέχοντας προηγμένες υπηρεσίες τηλεματικής και υπηρεσίες προστιθέμενης αξίας.
- Διάδοση των δυνατοτήτων του έργου στους διαχειριστές του ελληνικού δημόσιου τομέα. Οι εκπαιδευτικές δραστηριότητες που προβλέπονται στο πλαίσιο του έργου αποτελούν συστατικό όλων των εκπαιδευτικών δραστηριοτήτων που προβλέπονται για την αναβάθμιση του ανθρώπινου δυναμικού στον ελληνικό δημόσιο τομέα, είτε πρόκειται για εκπαίδευση στη χρήση πληροφοριακών συστημάτων είτε για απόκτηση βασικών δεξιοτήτων κατά τη χρήση. νέα τεχνολογία.
- Μέσω της λειτουργικής διασύνδεσης αυτών των συστημάτων, της εγκατάστασης ενός ιεραρχικού δικτύου διακομιστών και της διαχείρισης των τελικών χρηστών στη λογική ενός κλειστού περιβάλλοντος, χρησιμοποιούνται αποτελεσματικά τα συστήματα πληροφοριών του ελληνικού δημόσιου τομέα.
- Χρησιμοποιήστε εναλλακτικές πηγές πληροφοριών και αποφύγετε την επικάλυψη σε βάσεις δεδομένων και εγκαταστάσεις δικτύου.
- Αποτελεσματική διαχείριση της ροής δεδομένων των ελληνικών φορέων του δημόσιου τομέα και την κεντρική και κατακεντρωμένη υποστήριξη των εφαρμογών τηλεματικής.
- Μείωση του κόστους επικοινωνίας μεταξύ ελληνικών φορέων του δημόσιου τομέα, βελτιώνοντας παράλληλα την ταχύτητα και την ασφάλεια της κυκλοφορίας πληροφοριών.
- Μέσω της Ελληνικής Υπηρεσίας Δημόσιας Υπηρεσίας, οι υπηρεσίες που παρέχονται στους πολίτες έχουν αναβαθμιστεί πλήρως μέσω ενός αυτόματου και φιλικού προς το χρήστη συστήματος επεξεργασίας πληροφοριών και συναλλαγών.
- Οι πολίτες μπορούν εύκολα και γρήγορα να αναζητήσουν πληροφορίες που αποτελούν πηγή ελληνικών δημόσιων φορέων.
- Βελτίωση των υπηρεσιών πολιτών, ιδίως διαδικασιών που απαιτούν τη συμμετοχή πολλών υπηρεσιών. Ο απώτερος στόχος είναι η παροχή υπηρεσιών μίας στάσης.
- Επωφεληθείτε από τις δυνατότητες που προσφέρει η ελευθέρωση των τηλεπικοινωνιών και αναπτύξτε εναλλακτικούς τρόπους υλοποίησης και χρηματοδότησης έργων τηλεπικοινωνιών. Μειώστε το "ψηφιακό χάσμα" στην κοινωνία της πληροφορίας.



· Ταυτόχρονα, με την υλοποίηση του έργου, επιδιώξτε να αναπτύξετε τη βιομηχανία πληροφοριών και επικοινωνιών σε ένα περιβάλλον υγιούς ανταγωνισμού και πλήρους χρήσης των επενδύσεων τεχνολογίας πληροφοριών και επικοινωνιών. Η εμφάνιση μεγάλων έργων όπως το "ERMIS.GOV" αναμένεται να επηρεάσει την αγορά τηλεπικοινωνιών κυρίως όσον αφορά την παροχή ευρυζωνικών υπηρεσιών.

Νόμος 4727/2020

Ο πρόσφατα εκδοθείς νόμος αριθ. 4727/2020 (Επίσημη Εφημερίδα Α'184 / 23.09.2020) ασχολείται με την ψηφιακή διακυβέρνηση (Οδηγία 2016/2102 / Ενοποίηση της Ευρωπαϊκής Ένωσης) και τις ηλεκτρονικές επικοινωνίες (Οδηγία 2018/972 / Ενοποίηση της Ευρωπαϊκής Ένωσης)) - (εφεξής «κωδικός») - η εισαγωγή ενός νέου νομοθετικού συστήματος για το ψηφιακό περιβάλλον και τις ηλεκτρονικές επικοινωνίες. Οι διατάξεις των παραπάνω νόμων ισχύουν τόσο για ιδιώτες όσο και για εταιρείες, καθώς και για τις διατάξεις του άρθρου 14 του Ν. 4270/2014 (Α'143) Οργανισμοί γενικής κυβέρνησης, εξωτερικές νομικές οντότητες που ισχύουν για το δημόσιο δίκαιο (Ν.Π.Δ.Δ.) και μη δημόσιες επιχειρήσεις και οργανισμοί στο κεφάλαιο Α' του νόμου 3429/2005 (Α 314), ανεξάρτητα από το εάν εξαιρούνται από το πεδίο εφαρμογής για εφαρμοστέους σκοπούς, προκειμένου να διευκολυνθούν οι ανάγκες και οι διοικητικές διαδικασίες του.

Ταυτόχρονα, ο Κώδικας Ψηφιακής Διακυβέρνησης είναι σύμφωνος με τον ορισμό της ηλεκτρονικής υπογραφής στον Ευρωπαϊκό Κανονισμό 910/2014 (κανονισμός eIDAS) και καταργείται το προηγούμενο νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές, δηλαδή το Προεδρικό Διάταγμα αριθ. 150/2001 (Α'125). .

Ειδικότερα, αυτή η προδιαγραφή εισάγει τον ορισμό των εγκεκριμένων ηλεκτρονικών υπογραφών, εγκεκριμένων χρονικών σημείων, εγκεκριμένων και προηγμένων ηλεκτρονικών γραμματοσήμων, ηλεκτρονικών εγγράφων και εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης. Στο προηγούμενο πλαίσιο του Π.Δ. 150/2001, εισάγονται οι ορισμοί μόνο για απλές ηλεκτρονικές υπογραφές και για προηγμένες ηλεκτρονικές υπογραφές. Επομένως, παρέχονται τώρα τρεις τύποι ηλεκτρονικών υπογραφών, όπως περιγράφεται παρακάτω.



Ως "Ηλεκτρονική υπογραφή" αναφέρεται σε δεδομένα με ηλεκτρονική μορφή που συνδέονται με άλλα ηλεκτρονικά δεδομένα και χρησιμοποιείται από τον υπογράφοντα για υπογραφή.

Η "προηγμένη ηλεκτρονική υπογραφή" αναφέρεται σε μια υπογραφή που πληροί τις ακόλουθες απαιτήσεις:

1. έναν μοναδικό σύνδεσμο με τον υπογράφοντα ·
2. σε θέση να αναγνωρίσει τον υπογράφοντα ·
3. να χρησιμοποιήσει τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής που μπορεί να δημιουργήσει ο υπογράφων με τους ακόλουθους τρόπους:

Σύνδεση με τα υπογεγραμμένα δεδομένα που σχετίζονται με αυτό, έτσι ώστε να μπορεί να εντοπιστεί οποιαδήποτε μεταγενέστερη τροποποίηση των δεδομένων και η «εγκεκριμένη ηλεκτρονική υπογραφή» ορίζεται ως μια προηγμένη ηλεκτρονική υπογραφή που δημιουργήθηκε από μια εγκεκριμένη συσκευή δημιουργίας ηλεκτρονικής υπογραφής βάσει εγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής.

Επιπλέον, ως "προηγμένη ηλεκτρονική σφραγίδα" ορίζεται η ηλεκτρονική σφραγίδα που πληροί τις ακόλουθες απαιτήσεις:

1. Να υπάρχει μια μοναδική σύνδεση με τον υπογράφοντα
2. Να είναι σε θέση να αναγνωρίσει τον υπογράφοντα
3. Δημιουργήθηκε με ηλεκτρονικά δεδομένα δημιουργίας, ο υπογράφων μπορεί να χρησιμοποιήσει τα δεδομένα με μεγάλη εμπιστοσύνη υπό τον αποκλειστικό του έλεγχο
4. Χρειάζεται να υπάρχει σύνδεση με τα υπογεγραμμένα δεδομένα που σχετίζονται με αυτό.

Αυτό πραγματοποιείται, έτσι ώστε να μπορεί να εντοπιστεί οποιαδήποτε μεταγενέστερη τροποποίηση αυτών των δεδομένων και η "εγκεκριμένη ηλεκτρονική χρονική σήμανση" ορίζεται ως ηλεκτρονική χρονική σήμανση που πληροί τις ακόλουθες απαιτήσεις:



1. Να συνδέεται με την ημερομηνία και την ώρα με τα δεδομένα, για να αποκλειστεί εύλογα η πιθανότητα τροποποίησης δεδομένων που δεν μπορούν να εντοπιστούν.
2. Με βάση τη χρονολογική ακολουθία που σχετίζεται με το συντονισμένο καθολικό χρόνο.
3. Να φέρει ηλεκτρονική υπογραφή υψηλού επιπέδου ή ηλεκτρονική σφραγίδα υψηλού επιπέδου εγκεκριμένου παρόχου υπηρεσιών εμπιστοσύνης ή να την έχει υπογράψει με κάποια άλλη παρόμοια μέθοδο.

Είναι απαραίτητο να σημειωθεί ότι η εγκεκριμένη ηλεκτρονική υπογραφή φυσικών προσώπων και οι εγκεκριμένες ηλεκτρονικές σφραγίδες νομικών προσώπων και οντοτήτων έχουν τις θέσεις χειρόγραφων υπογραφών και πρωτότυπων γραμματοσήμων αντίστοιχα.

Επιπλέον, σύμφωνα με το Άρθρο 2 του Κώδικα, ως "αναγνωρισμένοι πάροχοι υπηρεσιών εμπιστοσύνης" ορίζονται ότι παρέχουν μία ή περισσότερες αναγνωρισμένες υπηρεσίες εμπιστοσύνης και έχουν λάβει την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) Ο σχετικός κατάλογος των εγκεκριμένων πάροχων υπηρεσιών εμπιστοσύνης που η Ελλάδα μπορεί να επιτρέψει την έκδοση εγκεκριμένων ηλεκτρονικών υπογραφών / γραμματοσήμων δημοσιεύεται στον ακόλουθο σύνδεσμο: https://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/ESignProviders.html.

Αξίζει να σημειωθεί ότι η ψηφιακή υπογραφή που εκδίδεται από την Ελληνική Αρχή Πιστοποίησης (Α.Π.Ε.Δ.) είναι ο πάροχος των υπηρεσιών εμπιστοσύνης στο ελληνικό κράτος, υπεύθυνη για την έκδοση και διαχείριση πιστοποιητικών σε όλες τις οντότητες του δημόσιου τομέα ή από διαπιστευμένους παρόχους υπηρεσιών εμπιστοσύνης στον ίδιο βαθμό αποτελεσματικότητας.

Επιπλέον, ο "Κώδικας", ιδίως τα άρθρα 13 έως 18, ορίζει τις διαδικασίες έκδοσης, διανομής, καταχώρησης και κατάθεσης που δεν επηρεάζουν τον παρόντα κανονισμό. Επίσης ορίζει τη νομιμότητα και την απόδειξη της αξίας δημόσιων ή ιδιωτικών ηλεκτρονικών εγγράφων και της εκτύπωσής τους για την ενιαία ψηφιακή πύλη για δημόσια διαχείριση.



Ειδικότερα, το άρθρο 13 των κατευθυντήριων γραμμών προβλέπει την έκδοση ηλεκτρονικών δημόσιων εγγράφων: "Όλες οι διαδικασίες για τα δημόσια ιδρύματα για τη διαχείριση δημόσιων εγγράφων, όπως σύνταξη, προώθηση υπογραφής, τοποθεσία υπογραφής, έκδοση, τιμολόγηση εισερχόμενων εγγράφων, εσωτερική και εξωτερική επεξεργασία, οι συμφωνίες και τα αρχεία τους μόνο μέσω ΤΠΕ. "

Τα ηλεκτρονικά δημόσια έγγραφα δημοσιεύονται σε μία από τις ακόλουθες μορφές:

1. Ως πρωτότυπο ηλεκτρονικό έγγραφο, με:

(α) εγκεκριμένη ηλεκτρονική σφραγίδα και

(β) ηλεκτρονική υπογραφή εγκεκριμένη από την αρμόδια αρχή

2. Ως ακριβές ηλεκτρονικό αντίγραφο, πρέπει να συνοδεύεται από:

α) εγκεκριμένη ηλεκτρονική σφραγίδα,

β) εγκεκριμένη ηλεκτρονική υπογραφή του ιδρύματος που είναι υπεύθυνο για την έκδοση του αντιγράφου, λεπτομέρειες του ιδρύματος που είναι ο τελικός υπογράφων για την υπογραφή του εγγράφου και

3. Ως ψηφιοποιημένο ηλεκτρονικό αντίγραφο, με:

α) εγκεκριμένη ηλεκτρονική σφραγίδα ώρας

β) ηλεκτρονική υπογραφή εγκεκριμένη από τον οργανισμό του ιδρύματος που χρησιμοποιεί ΤΠΕ για ψηφιοποίηση ή αναπαραγωγή σύμφωνα με τις παραπάνω παραγράφους · και

γ) πιστοποιητικό ταυτότητας, βιβλία και έντυπα έγγραφα.

Παρομοίως, προηγμένες ή εγκεκριμένες ηλεκτρονικές υπογραφές ή προηγμένες ή εγκεκριμένες ηλεκτρονικές σφραγίδες μπορούν να χρησιμοποιηθούν για την έκδοση οποιουδήποτε είδους πιστοποιητικών και πιστοποιήσεων χωρίς να επηρεάζεται η δημόσια διοίκηση μιας ενιαίας ψηφιακής πύλης.

Πρέπει να επισημανθεί ότι τα πρωτότυπα ηλεκτρονικά δημόσια έγγραφα και τα ακριβή ηλεκτρονικά αντίγραφα και τα ψηφιοποιημένα ηλεκτρονικά αντίγραφα, καθώς και η



πιστοποίηση του άρθρου 13, παράγραφος 6 του κώδικα, έχουν το ίδιο νομικό αποτέλεσμα με τα χειρόγραφα δημόσια έγγραφα. Η υπογραφή και η σφραγίδα είναι υποχρεωτικά αποδεκτά από οργανισμούς του δημόσιου τομέα, όλα τα δικαστήρια και εισαγγελείς, φυσικά πρόσωπα ή νομικά πρόσωπα.

Οι εθνικοί οργανισμοί του δημόσιου τομέα, τα δικαστήρια και οι δικαστές σε όλα τα επίπεδα, καθώς και τα φυσικά πρόσωπα, τα νομικά πρόσωπα πρέπει υποχρεωτικά να αποδεχθούν έντυπα υλικά από πρωτότυπα ηλεκτρονικά δημόσια έγγραφα ή ηλεκτρονικά ακριβή αντίγραφα ή ψηφιακά ηλεκτρονικά αντίγραφα. Εάν η ακρίβεια και η εγκυρότητα της εκτύπωσης ΤΠΕ μπορεί να επαληθευτεί, ειδικά το πρωτότυπο ηλεκτρονικό δημόσιο έγγραφο ή το ακριβές ηλεκτρονικό αντίγραφο ή το ψηφιακό ηλεκτρονικό αντίγραφο με ένα μοναδικό αναγνωριστικό ταυτότητας και χώρα. Εάν η ακρίβεια και η εγκυρότητα του παραπάνω περιεχομένου δεν μπορεί να επιβεβαιωθεί, οποιαδήποτε ρυθμιστική αρχή ή κέντρο εξυπηρέτησης πολιτών (ΚΕΠ) ή δικηγόρος θα πρέπει να επιβεβαιώσει το έντυπο αντίγραφο.

Επιπλέον, το άρθρο 15 του κώδικα ορίζει ότι τα ηλεκτρονικά ιδιωτικά έγγραφα που εκδίδονται από φυσικά πρόσωπα ή νομικά πρόσωπα ή νομικά πρόσωπα που χρησιμοποιούν εξουσιοδοτημένες ηλεκτρονικές υπογραφές ή εγκεκριμένες ηλεκτρονικές σφραγίδες πρέπει να εκδίδονται από φορείς του δημόσιου τομέα σε ολόκληρη τη χώρα. Δικαστήρια και εισαγγελείς και φυσικά ή νομικά πρόσωπα δέχονται άτομα ή νομικά πρόσωπα για ηλεκτρονική κυκλοφορία. Οι υπηρεσίες του δημόσιου τομέα, τα δικαστήρια και οι εισαγγελικές αρχές σε όλα τα επίπεδα της χώρας και φυσικά ή νομικά πρόσωπα πρέπει να αποδεχθούν την εκτύπωση ηλεκτρονικών εγγράφων στην παράγραφο 1. Αυτό γίνεται επαληθεύοντας την ταυτότητα του περιεχομένου του έντυπου εγγράφου με ένα ηλεκτρονικό ιδιωτικό έγγραφο.

Επιπλέον, το άρθρο 17 του «Κώδικα» για την ηλεκτρονική κυκλοφορία ηλεκτρονικών δημόσιων εγγράφων εντός του ίδιου οργανισμού ορίζει:

1.« Σε κλειστό σύστημα πληροφοριών (όπως το εσωτερικό σύστημα μεταφοράς ηλεκτρονικών εγγράφων, (SIDE), η ηλεκτρονική χρονική σήμανση και η ηλεκτρονική σφραγίδα υψηλού επιπέδου ή εγκεκριμένη του ιδρύματος ή η ηλεκτρονική υπογραφή υψηλού επιπέδου ή εγκεκριμένη από την αρμόδια αρχή.



2. Η χρήση του εσωτερικού συστήματος επεξεργασίας εγγράφων βασίζεται στην αυθεντικότητα κάθε χρήστη. "

Τέλος, ως «έλεγχος ταυτότητας» στο πλαίσιο του προαναφερθέντος «Κώδικα» ορίζεται η ηλεκτρονική διαδικασία επαλήθευσης σε οποιονδήποτε ειδικών χαρακτηριστικών φυσικών / νομικών προσώπων ή φυσικών/νομικών προσώπων με βάση εκδοθέντα πιστοποιητικά και τα «κουπόνια» ορίζονται ως εγγυήσεις. Πληροφορίες που παρέχονται από φυσικά ή νομικά πρόσωπα ή νομικά πρόσωπα που χρησιμοποιούν ψηφιακές δημόσιες υπηρεσίες για την επαλήθευση της ταυτότητάς τους.

Για να αποσαφηνιστεί ο παραπάνω ορισμός, οι "χρήστες ψηφιακών δημόσιων υπηρεσιών" αναφέρονται σε φυσικά πρόσωπα ή νομικά πρόσωπα που χρησιμοποιούν ψηφιακές δημόσιες υπηρεσίες. Οι χρήστες ψηφιακών δημόσιων υπηρεσιών αναφέρονται επίσης σε ιδιωτικούς υπαλλήλους και υπαλλήλους δημόσιων υπηρεσιών που τους χρησιμοποιούν κατά την εκτέλεση των καθηκόντων τους, ενώ οι «δημόσιες υπηρεσίες» αναφέρονται σε υπηρεσίες γενικής κυβέρνησης σύμφωνα με το άρθρο 14 του νόμου 4270/2014 και δεν υπόκεινται στο δημόσιο δίκαιο (Ν.Π.Δ.Δ.) Νομικές οντότητες υπό δικαιοδοσία και άλλες οντότητες από δημόσιες επιχειρήσεις και οργανισμούς που καλύπτονται από το Κεφάλαιο Α του Ν. 3429/2005, ανεξάρτητα από το εάν εξαιρούνται από το πεδίο εφαρμογής τους.



ΚΕΦΑΛΑΙΟ 3^ο Εφαρμογές ηλεκτρονικών υπογράφων στον ιδιωτικό τομέα

Στον ιδιωτικό τομέα η εφαρμογή ηλεκτρονικών υπογραφών που επιλέχθηκε να σχολιαστεί είναι η ηλεκτρονική τιμολόγηση καθώς θεωρείται σημαντική και εξαιρετικά ενδιαφέρονσα.

Ηλεκτρονική τιμολόγηση (e-Invoicing)

Με την έλευση της ηλεκτρονικής εποχής (ηλεκτρονική εποχή), αλλά κυρίως λόγω της αναγνώρισης και της εισαγωγής του Διαδικτύου ως εναλλακτικής μεθόδου συναλλαγών, οι εμπορικές προσπάθειες της νέας ηλεκτρονικής βιομηχανίας (ηλεκτρονική βιομηχανία) έχουν στραφεί ακόμη και στη χρήση νέων τεχνολογιών στην επιχείρηση "Παραδοσιακές" περιοχές που δεν θέλουν να τροποποιήσουν. Ένα τυπικό παράδειγμα αυτού του τύπου επιχειρηματικής μονάδας είναι η τιμολόγηση.

Στο σύντομο ιστορικό των διαδικτυακών υπηρεσιών, σχετικά νέες τιμές έχουν αναπτυχθεί σε ηλεκτρονική μορφή και η μορφή αλλά και η μέθοδος τους δεν έχουν ακόμη καθοριστεί πλήρως. Ο κύριος λόγος για τη διαφορά ώρας είναι η έλλειψη κατάλληλου νομικού πλαισίου και ολοκληρωμένων τεχνικών λύσεων, οι οποίες εστιάζονται στις ειδικές ανάγκες των ηλεκτρονικών τιμολογίων και στις εγγυήσεις που απαιτούνται για την ανταλλαγή ηλεκτρονικών τιμολογίων.

Ο Νόμος 4727/2020 (ΦΕΚ Α' 184/23.09.2020) για την Ψηφιακή Διακυβέρνηση (ενσωμάτωση της Οδηγίας 2016/2102/ΕΕ) και για τις Ηλεκτρονικές Επικοινωνίες (ενσωμάτωση της Οδηγίας 2018/972/ΕΕ), εξουσιοδοτεί όλες τις εταιρείες εντός της ΕΕ να εκδίδουν ηλεκτρονικά τιμολόγια και δελτία αποστολής, με απώτερο στόχο την αντικατάσταση των αντίστοιχων έντυπων εγγράφων. Αυτός ο κανονισμός θα εφαρμοστεί σε όλες τις ευρωπαϊκές χώρες από το 2020.

Η πραγματοποίηση ηλεκτρονικών τιμολογίων μελετάται σε πανευρωπαϊκό φάσμα. Η ηλεκτρονική έκδοση τιμολογίων πρέπει να συμμορφώνεται με τις παραπάνω οδηγίες και πρέπει να είναι αποδεκτή από όλα τα κράτη μέλη της ΕΕ, δια λειτουργική, ασφαλή και οικονομικά αποδεκτή. Ορίζει επίσης ότι όλα τα τιμολόγια που διαβιβάζονται ηλεκτρονικά θεωρούνται έγκυρα και αποδεκτά, αλλά πρέπει να πληρούνται οι ακόλουθες δύο προϋποθέσεις:



1. Ο παραλήπτης του τιμολογίου πρέπει να συμφωνήσει και να αποδεχτεί τις σχετικές μεθόδους, και

2. Απαιτείται η χρήση ψηφιακών υπογραφών ή συστημάτων EDI (Ηλεκτρονική ανταλλαγή δεδομένων) για την αποστολή και λήψη τιμολογίων σε ασφαλές διαδικτυακό περιβάλλον.

Όσον αφορά την πρώτη προϋπόθεση, η συγκατάθεση του παραλήπτη μπορεί να ληφθεί μέσω προηγούμενης εμπορικής σύμβασης. Όσον αφορά τη δεύτερη συνθήκη, ισχύουν οι ακόλουθες προϋποθέσεις: η ηλεκτρονική υπογραφή είναι δεδομένα σε ψηφιακή μορφή, τα οποία συνοδεύονται ή σχετίζονται λογικά με άλλα ηλεκτρονικά δεδομένα και χρησιμοποιείται ως μέθοδος για την απόδειξη της αυθεντικότητας. Συνδέεται σαφώς και προσδιορίζεται συγκεκριμένα η υπογραφή αφού εξοικειωθούν με το νέο νομικό πλαίσιο για την απαραίτητη χρονική περίοδο. Ειδικοί αναλυτές ηλεκτρονικών υπηρεσιών συμφώνησαν ότι η πρώτη αντίδραση ήταν ιδιαίτερα ενθαρρυντική.

Τώρα, γενικά πιστεύεται ότι τα χαρακτηριστικά των ηλεκτρονικών τιμολογίων είναι πολύ θετικές δυναμικές, οι οποίες απορρέουν από το ευρύ φάσμα των πλεονεκτημάτων και των ευκαιριών που παρέχουν αυτές οι υπηρεσίες.

Αυτά τα πλεονεκτήματα επικεντρώνονται κυρίως στην πλήρη αυτοματοποίηση και ενοποίηση των διαδικτυακών συναλλαγών, ωφελώντας τόσο τους προμηθευτές όσο και τους λιανοπωλητές. Επιπλέον, μειώνει το χρόνο παράδοσης των εγγράφων, μειώνει το κόστος έκδοσης τιμολογίων και προκαλεί δυσλειτουργίες λόγω της εμπλοκής ανθρώπινων παραγόντων στις παραδοσιακές υπηρεσίες τιμολογίου (όπως απώλεια, φθορά κ.λπ.). Ταυτόχρονα, ο διαθέσιμος χρόνος των σχετικών υπηρεσιών έχει επίσης αυξηθεί. Μπορεί επίσης να γίνει εκτός των ωρών εργασίας ανθρώπινου δυναμικού. Τα παραπάνω δεδομένα ισχύουν για εταιρείες και οργανισμούς που επιλέγουν ηλεκτρονικά τιμολόγια, τα οποία έχουν συγκριτικό πλεονέκτημα έναντι των εταιρειών και οργανισμών που τηρούν το μοντέλο «παραδοσιακό τιμολόγιο».

Ωστόσο, παρόλο που οι μικρές και μεσαίες επιχειρήσεις μπορούν να αποκτήσουν τα οφέλη από τη χρήση ηλεκτρονικών τιμολογίων, συνήθως δεν έχουν τους πόρους για την εφαρμογή τους. Το Πανευρωπαϊκό Εμπορικό Επιμελητήριο έχει συνειδητοποιήσει αυτή την ανάγκη και επιδιώκει να μελετήσει την επιτυχή εγκατάσταση μιας ασφαλούς



υπηρεσίας ηλεκτρονικών τιμολογίων χαμηλού κόστους για να διευκολύνει τις τεχνικές λύσεις των μελών του και να μελετήσει πιθανά επιχειρηματικά μοντέλα που μπορούν να παρέχουν αυτήν την υπηρεσία.

Σήμερα, οι περισσότερες εφαρμογές ηλεκτρονικής χρέωσης βασίζονται στο EDI(ένα πρότυπο που υποστηρίζεται από την οδηγία και ανταλλάσσει δεδομένα από ERP σε ERP, χωρίς να υπάρχει ανάγκη χειρονακτικής καταχώρησης). Ωστόσο, αυτές οι υλοποιήσεις έχουν σημαντικές ελλείψεις, όπως υψηλό κόστος συντήρησης και έλλειψη υποστήριξης για νέα πρότυπα ανταλλαγής πληροφοριών. Επιπλέον, οι υπάρχουσες ηλεκτρονικές λύσεις τιμολογίων προσπαθούν να ικανοποιήσουν τις απαιτήσεις με διάφορους τρόπους και να διασφαλίσουν τη συμβατότητα με τα υπάρχοντα λογιστικά συστήματα πληροφοριών. Τα περισσότερα περιλαμβάνουν μετατροπείς από τη μία φόρμα στην άλλη, διαχείριση τιμολογίων τρίτων, ολοκληρωμένες εφαρμογές με ευρύτερο φάσμα λειτουργιών εκτός από την ανταλλαγή τιμολογίων, τη χρήση κωδικών ελέγχου ταυτότητας μηνυμάτων και SSL για ασφαλή μεταφορά τιμολογίων.

Ωστόσο, όλες οι υπάρχουσες λύσεις πληρούν μόνο ένα υποσύνολο των απαιτήσεων ηλεκτρονικού τιμολογίου και τα χαρακτηριστικά ασφαλείας ορισμένων λύσεων είναι αμφισβητήσιμα. Πιο συγκεκριμένα, αυτός ο τεχνικός τομέας δεν χρειάζεται να αποδείξει την εφαρμογή μέτρων που συνδυάζουν όλες τις απαιτήσεις της οδηγίας, αυτά τα μέτρα βασίζονται σε ένα ευρύ φάσμα προτύπων για να διασφαλιστεί η δια λειτουργικότητα (βασισμένη σε χαμηλού κόστους υποδομή ανοικτού δικτύου που μπορεί να ικανοποιεί όλες τις απαιτήσεις) θέματα πολιτικής.

Το SELIS είναι μια διασυνοριακή υπηρεσία για την ασφαλή ανταλλαγή ηλεκτρονικών τιμολογίων. Βασίζεται σε μια καινοτόμο αρχιτεκτονική που χρησιμοποιεί τα πιο προηγμένα πρότυπα για την ασφαλή παροχή δια λειτουργικών υπηρεσιών (όπως υπηρεσίες Web, XML, PPC) σύμφωνα με τις απαιτήσεις του κοινοτικού πλαισίου. Η υπηρεσία SELIS επιτρέπει την ενοποίηση με τα υπάρχοντα λογιστικά συστήματα πληροφοριών που μπορούν να χρησιμοποιούν οι οργανισμοί όταν χρησιμοποιούν XML, αλλά μπορούν επίσης να χρησιμοποιηθούν ως αυτόνομη ηλεκτρονική εφαρμογή διαχείρισης τιμολογίων για μικρούς χρήστες.



Νομικό πλαίσιο

Ο Αναπληρωτής Υπουργός Οικονομικών και ο Διευθυντής της Ανεξάρτητης Υπηρεσίας Δημοσίων Εσόδων υπέγραψαν κοινή απόφαση με την οποία ενεργοποίησαν την ψηφιακή μετάδοση στην πλατφόρμα Ηλεκτρονικών Βιβλίων myDATA. Η απόφαση αναμένεται να δημοσιευτεί στην εφημερίδα της κυβέρνησης. Το Υπουργείο Οικονομικών και το ΑΑΔΕ χρησιμοποιούν τις διεθνείς βέλτιστες πρακτικές και με τον μόνιμο στόχο ενοποίησης της εμπιστοσύνης μαζί τους, για την πραγματοποίηση πρωτοποριακών ψηφιακών μεταρρυθμίσεων στις εμπορικές σχέσεις με τη χώρα. επιχείρηση.

Η απόφαση θέτει ένα νέο πλαίσιο στο οποίο η εταιρεία θα μεταφέρει ηλεκτρονικά δεδομένα από τα λογιστικά της δεδομένα και τα βιβλία λογαριασμών στην ΑΑΔΕ ανεξάρτητα από το μέγεθός της και τη μέθοδο έκδοσης και συντήρησης λογιστικών αρχείων (βιβλιογραφία).

Η απόφαση καθορίζει το πεδίο εφαρμογής, τις εξαιρέσεις, τα δεδομένα που πρέπει να διαβιβάζονται, τον χρόνο, τη μέθοδο μετάδοσης και τις συγκεκριμένες υποχρεώσεις της εταιρείας.

Η ανάπτυξη του έργου μετάδοσης δεδομένων my DATA στην πλατφόρμα e-book θα πραγματοποιηθεί σε φάσεις για να παρέχει τον απαραίτητο χρόνο για την ηλεκτρονική επικοινωνία της εταιρείας με τα Συστήματα Πληροφοριών ΑΑΔΕ.

- Για τις εταιρείες που επιλέγουν να χρησιμοποιούν ηλεκτρονικά τιμολόγια μέσω παρόχων ως μέθοδο τιμολόγησης, η δυνατότητα ηλεκτρονικής διαβίβασης δεδομένων για αποδείξεις θα ξεκινήσει στις 20 Ιουλίου 2020.
- Για εταιρείες που δεν επιλέγουν ηλεκτρονικά τιμολόγια μέσω παρόχων και δημοσιεύουν έγγραφα χειροκίνητα ή ηλεκτρονικά μέσω διαδικασιών διαχείρισης επιχειρήσεων (επιχείρηση / λογιστική, ERP), η υποχρέωση διαβίβασης δεδομένων παραλαβής θα αρχίσει την 1η Οκτωβρίου 2020.
- Από την 1η Οκτωβρίου 2020, τα δεδομένα λιανικής θα διαβιβάζονται. Για προϊόντα λιανικής που είναι υποχρεωμένα να χρησιμοποιούν το ταμειακό μητρώο (ΦΗΜ), έως ότου εκδοθεί η νέα απόφαση του Υπουργείου Οικονομικών σύμφωνα με τις συστάσεις του ΑΑΔΕ, η κεντρική μεταφορά θα πραγματοποιείται κάθε μήνα, εκτός εάν υπάρχει



υποχρέωση απευθείας σύνδεσης ΦΗΜ και ΑΑΔΕ και μεταφορά τους σύμφωνα με είδη λιανικής . Για προϊόντα λιανικής που εκδίδονται χωρίς υποχρεώσεις ΦΗΜ, παρέχεται η μετάδοση κάθε προϊόντος λιανικής από την 1η Ιανουαρίου 2021.

- Από την 1η Οκτωβρίου 2020, θα ξεκινήσει η ηλεκτρονική διαβίβαση των χαρακτηριστικών του εγγράφου που θα έχουν ληφθεί από όλες τις εταιρείες (χρεώσεις) από την ημερομηνία αυτή.
- Έως τις 31 Δεκεμβρίου 2020, η εταιρεία πρέπει να διαβιβάζει τα δεδομένα όλων των δημοσιευμένων εσόδων της, από την 1η Ιανουαρίου 2020 έως την ημερομηνία της πρώτης διαβίβασης, όπως περιγράφεται παραπάνω,
- Έως τις 28 Φεβρουαρίου 2021, οι εταιρείες πρέπει να υποβάλουν το επίπεδο των εσόδων εξόδων που έχουν ληφθεί και εκδοθεί από την 1η Ιανουαρίου 2020 έως τις 30 Σεπτεμβρίου 2020.

Μια σημαντική παράμετρος για την σωστή καταγραφή της λογιστικής εικόνας της εταιρείας στα myDATA είναι ότι για τις εταιρείες που έχουν την αντίστοιχη υποχρέωση δήλωσης ετήσιου φόρου εισοδήματος, είναι υποχρεωμένες να περάσουν την ταξινόμηση εξόδων από τον λογιστή.

Ταυτόχρονα, προκειμένου να ενθαρρυνθούν οι εταιρείες να επιλέξουν ηλεκτρονικά τιμολόγια από παρόχους ως μέθοδο έκδοσης εγγράφων, το Υπουργείο Οικονομικών και η Ανεξάρτητη Διοίκηση Δημοσίων Εσόδων έχουν διατυπώσει μια σειρά εταιρικών κινήτρων, τα οποία θα περιληφθούν σε επερχόμενο νομοσχέδιο.

Απαιτήσεις ασφαλείας

Προς το παρόν, θα εισαχθούν περαιτέρω οι βασικές απαιτήσεις ασφαλείας του συστήματος ηλεκτρονικών τιμολογίων. Αυτές οι απαιτήσεις μπορούν να συνοψιστούν ως εξής:

- Επαλήθευση προέλευσης για να διασφαλιστεί ότι ο εκδότης του τιμολογίου είναι πράγματι η πραγματική ταυτότητα που ισχυρίζεται. Η φορολογική αρχή πρέπει να επιβεβαιώσει τους φορολογούμενους που συμμετέχουν στη συναλλαγή με ηλεκτρονικό τιμολόγιο, προκειμένου να προσδιορίσει σαφώς τα μέρη που εμπλέκονται στη φορολογητέα συναλλαγή.



- Η ακεραιότητα του περιεχομένου τιμολογίου για να διασφαλιστεί ότι το τιμολόγιο δεν θα αλλάξει σκόπιμα ή ακούσια κατά τη διάρκεια της μετάδοσης ή αποθήκευσης, έτσι ώστε τα ενδιαφερόμενα μέρη να έχουν πλήρη εμπιστοσύνη στο περιεχόμενο του τιμολογίου.
- Αποποίηση ευθυνών για να διασφαλιστεί ότι ούτε ο αποστολέας ούτε ο παραλήπτης μπορούν να αρνηθούν την ανταλλαγή τιμολογίων που έχουν συμβεί.
- Εμπιστευτικότητα / ακεραιότητα, για να διασφαλιστεί ότι κανένας από τον αποστολέα και τον καθορισμένο παραλήπτη δεν μπορεί να διαβάσει το ηλεκτρονικό τιμολόγιο.
- Η πληρότητα της ακολουθίας τιμολογίου. Ο σκοπός αυτής της απαίτησης είναι να αποφευχθούν κενά στα τιμολόγια και να ενισχυθεί ο έλεγχος.
- Διαθεσιμότητα, έτσι ώστε οι εταιρείες να μπορούν να χρησιμοποιούν υπηρεσίες ηλεκτρονικών τιμολογίων ανά πάσα στιγμή χωρίς να προκαλούν προβλήματα στις λογιστικές πρακτικές.
- Ηλεκτρονική αποθήκευση ηλεκτρονικών τιμολογίων. Οι συνθήκες ηλεκτρονικής αποθήκευσης ηλεκτρονικών τιμολογίων και οι τεχνικές απαιτήσεις των ηλεκτρονικών συστημάτων αποθήκευσης αποτελούν μέρος των απαιτήσεων ασφάλειας για ηλεκτρονικά τιμολόγια. Σύμφωνα με τις κοινοτικές οδηγίες ηλεκτρονικού τιμολογίου, η αυθεντικότητα, η πληρότητα και η αναγνωσιμότητα πρέπει να είναι εγγυημένα καθ' όλη τη διάρκεια της περιόδου αποθήκευσης.



Συμπεράσματα

Τα ηλεκτρονικά τιμολόγια έχουν αναμφίβολα εμπορικά οφέλη για τις εταιρείες και τους οργανισμούς που το υιοθετούν, είτε πρόκειται για τη βελτίωση της αποτελεσματικότητας των τιμολογίων επεξεργασίας δεδομένων, είτε από την άποψη της διαχείρισης πόρων. Επίσης στην Ευρώπη, ακόμη και σε διασυνοριακές συναλλαγές, θα επιτρέψει τον αποτελεσματικό και ακριβή έλεγχο των εσόδων από ΦΠΑ. Η ευρωπαϊκή οδηγία 2001/115 / ΕΚ έχει ήδη δώσει την ευρωπαϊκή κατεύθυνση για την έγκριση, ανάπτυξη και αποδοχή υπηρεσιών ηλεκτρονικών τιμολογίων.

Από την πλευρά της εταιρείας, η προοπτική της ηλεκτρονικής τιμολόγησης μπορεί να υποστηρίξει την τάση: Μέσα σε λίγα χρόνια, οι περισσότερες μεγάλες και μικρές επιχειρήσεις θα επιδιώξουν να συνεργαστούν με μικρές και μεσαίες επιχειρήσεις που μπορούν να συμμετάσχουν στη διαδικασία ηλεκτρονικής τιμολόγησης και να αποφύγουν τη συνεργασία. Και όσοι θα συνεχίσουν να χρησιμοποιούν το "παραδοσιακό" μοντέλο. Επομένως, η υιοθέτησή του από εμπορικά μέσα θεωρείται απαραίτητη προϋπόθεση για τη διατήρηση ή ακόμη και τη βελτίωση της ανταγωνιστικότητας. Μπορεί ακόμη να φανεί ότι λύσεις που μπορούν να ικανοποιήσουν όλες τις απαιτήσεις του επιχειρηματικού κόσμου και τους νόμους, όπως η υπηρεσία SELIS(η μεγαλύτερη εταιρεία logistics στην Ελλάδα) που παρέχεται παραπάνω, μπορούν να εισαχθούν με επιτυχία στην αγορά.



Βιβλιογραφία

1. Δελούκα-Ιγγλέση Κ. (2015). Νομικά θέματα Ηλεκτρονικού Εμπορίου. Β΄ Έκδοση. Αθήνα-Θεσσαλονίκη. Εκδόσεις Σάκκουλα.
2. Ζέκος Γ. (2017) Διαδίκτυο, Η/Υ & τηλεπικοινωνίες στο ελληνικό δίκαιο, Εκδόσεις Σάκκουλας, Αθήνα-Θεσσαλονίκη
3. Ιγγλεζάκης Ι. (2008). Δίκαιο της Πληροφορικής. Αθήνα-Θεσσαλονίκη. Εκδόσεις Σάκκουλα.
4. Ιγγλεζάκης Ι. (2009). Το δίκαιο του ηλεκτρονικού εμπορίου[Επιτομή]. Αθήνα – Θεσσαλονίκη. Εκδόσεις Σάκκουλα.
5. Ιγγλεζάκης Ι. (2012). Νομική Πληροφορική. Η εφαρμογή των τεχνολογιών πληροφορικής και επικοινωνιών στη νομική πράξη. Αθήνα – Θεσσαλονίκη. Εκδόσεις Σάκουλα.
6. Ιγγλεζάκης Ι., (2018). Δίκαιο πληροφορικής, 3η έκδ., εκδόσεις Αθήνα-Θεσσαλονίκη
7. Κόμνιος Κομνηνός, (2017) Το νέο ευρωπαϊκό νομοθετικό πλαίσιο για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης - Συναφή ζητήματα δικαίου απόδειξης, Εφαρμογές Αστικού Δικαίου & Πολιτικής Δικονομίας 6 σ. 498-510.
8. Καραδημητρίου Κ. (2008). Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο. Θεσσαλονίκη. Εκδόσεις Σάκκουλα.
9. Κουμεντάκης Σταύρος, (2019) «Η 4η Βιομηχανική Επανάσταση - Ρυθμίζεται, άραγε, η ανάπτυξη;», Capital.gr, διαθέσιμο στην ιστοσελίδα <https://www.capital.gr/arhtra/3385609/i-4i-biomixaniki-epanastasi-ruthmizetai-arage-ianaptuxi> (ημερομηνία προσπέλασης: 28-05-2020)
10. Λιναρίτης Ι. , (2002). Η νομοθετική ρύθμιση των ηλεκτρονικών υπογραφών μετά την ενσωμάτωση της Οδηγίας 99/93 της Ευρωπαϊκής Ένωσης στο ελληνικό δίκαιο με το ΠΔ 150/2001, ΔΕΕ
11. Χριστοδούλου Κ. (2013). Επιτομή Ηλεκτρονικού Αστικού Δικαίου, δεύτερη αναθεωρημένη έκδοση. Αθήνα-Κομοτηνή. Εκδόσεις Αντ. Σάκκουλα.



Ξενόγλωσση

1. Andress J. (2014) The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice 2nd Edition. Oxford: Elsevier Inc.
2. Bose S. and Vijayakumar P. (2016) Cryptography and Network Security. Chennai: Pearson India Education Services Pvt.

Νομολογία

ΕφΑθηνών 46/2014 ΔΕΕ 4/2014, σ. 373

ΕφΑθηνών 32/2011, ΔΕΕ 5/2011 σ. 591

ΜονΠρΑθ 1327/2001, ΔΕΕ 4/2001 με παρατηρήσεις Κοσούλη, σ. 377 = Δ 32 (2001) με παρατηρήσεις Μπέη Κ, Σ. 457

1Π.ΔΙ 502001: Προσαρμογή στην Οδηγία 99/93ΕΚ Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

Άρθρα

- <http://www.eett.gr>

- [http:// www.acci.gr](http://www.acci.gr)

- [http:// www.ΣΥΖΕΥΞΙΣ.gov.gr](http://www.ΣΥΖΕΥΞΙΣ.gov.gr)

-[http:// www.euro2day.gr/articles/90389/](http://www.euro2day.gr/articles/90389/)

-[http:// www.ciscoexpo.gr/2006/downloads/0902/omega/stuer.Π.Α.f](http://www.ciscoexpo.gr/2006/downloads/0902/omega/stuer.Π.Α.f)

-http://www.go-online.gr/ebusiness/specials/article.html?article_id=1355



Διπλωματική Εργασία

Τίτλος Μελέτης: Ψηφιακή Υπογραφή με βάση το Ελληνικό και Ευρωπαϊκό Νομοθετικό Πλαίσιο –
Ο Βαθμός Ανάπτυξης των Ψηφιακών Υπογραφών στον Δημόσιο και Ιδιωτικό Τομέα
Κοκώνη Αρβανίτη

- http://en.wikipedia.org/wiki/Electronic_Data_Interchange
- [**http://www.ase.gr/SmartAccess/files/Eisagwgi_EPMHS-1_0.Π.Δ.φ**](http://www.ase.gr/SmartAccess/files/Eisagwgi_EPMHS-1_0.Π.Δ.φ)
- http://www.ict.etsi.org/EESSI_home.html.