ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΚΑΙ ΠΡΟΕΔΡΙΚΟ ΔΙΑΤΑΓΜΑ 150/2001

Μιρτζάνης Εμμανουήλ, **Ασφάλεια Εφαρμογών Διαδικτύου**, Τηλ: **210 49 50 393**
Έκδοση Ψηφιακών Πιστοποιητικών για Ψηφιακή Υπογραφή – Εκπαίδευση

Το **Προεδρικό Διάταγμα 150/2001** στο **άρθρο 3 παρ. 1**, καθορίζει με σαφήνεια ποια ηλεκτρονική υπογραφή σε ηλεκτρονικά έγγραφα ή σε η-μηνύματα (email) επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.

Αυτή είναι η "**Προηγμένη Ηλεκτρονική Υπογραφή**" (ΠΔ 150/2001 άρθρο 2, παρ. 2 - κανονισμός 910-2014 ΕΚ άρθρο 3 παρ. 11, άρθρο 26) για να την οποία ισχύουν οι παρακάτω δύο προϋποθέσεις:

1) το πιστοποιητικό (ψηφιακή ταυτότητα) του υπογράφοντος, που έχει εκδοθεί γι αυτό το σκοπό, θα πρέπει να είναι "**Αναγνωρισμένο (Εγκεκριμένο)**", δηλαδή θα πρέπει να πληροί τις απαιτήσεις του Παραρτήματος Ι και να έχει εκδοθεί από **εμπιστευμένο Πάροχο Υπηρεσιών Πιστοποίησης** που πληροί τους όρους του Παρατήματος ΙΙ και συμμορφώνεται με τους ισχύοντες κανονισμούς για την αξιοπιστία των παρεχομένων υπηρεσιών του.

2) το λογισμικό που δημιουργεί την υπογραφή θα πρέπει να είναι αποθηκευμένο σε **Ασφαλή (Εγκεκριμένη) Διάταξη Δημιουργίας Υπογραφής (ΑΔΔΥ, USB token, στικάκι)** που θα πρέπει να πληροί τις απαιτήσεις του Παραρτήματος ΙΙΙ και τις τρέχουσες τεχνολογικές προδιαγραφές ασφαλείας. Θα πρέπει να βρίσκεται δε στην αποκλειστική κατοχή του υπογράφοντος. **Δεν επιτρέπεται η έκθεσή της σε τρίτους**.

Σε αυτή την περίπτωση η Προηγμένη Ηλεκτρονική Υπογραφή ονομάζεται **Εγκεκριμένη (κανονισμός 910-2014 ΕΚ, άρθρο 3, παρ. 12)**

Η τεχνολογία που χρησιμοποιείται για την **Εγκεκριμένη Ηλεκτρονική Υπογραφή** και τα πιστοποιητικά υπογραφής και κρυπτογράφησης (**Υποδομή Δημόσιου Κλειδιού**), με νομική ισχύ αυτή της παραγράφου 1 του άρθρου 3 του ΠΔ 150/2001 έχει στην κοινωνική και επαγγελματική ζωή μας τα κάτωθι αποτελέσματα:

1. Αυθεντικοποιεί κάθε υπογεγραμμένο ηλεκτρονικό έγγραφο ή η-μήνυμα (email) με υψηλό βαθμό ασφάλειας και με έλεγχο ισχύος του πιστοποιητικού (ψηφιακής ταυτότητας) του υπογράφοντος κάθε φορά που εμφανίζεται σε έναν Ηλεκτρονικό Υπολογιστή (Η/Υ).

2. Ελέγχει την **ακεραιότητα** (μη παραποίηση) του περιεχομένου κειμένου, το οποίο έχει υπογραφεί (σε η-έγγραφο ή η-μήνυμα) , κάθε φορά που εμφανίζεται σε έναν Η/Υ.

3. Δίνει την δυνατότητα κρυπτογράφησης (**εμπιστευτικότητα**) σε η-έγγραφα και η-μηνύματα, το περιεχόμενο των οποίων δεν πρέπει να είναι προσβάσιμο σε τρίτους παρά μόνο στον αρμόδιο παραλήπτη.

4. Ο υπογράφων ηλεκτρονικό έγγραφο ή η-μήνυμα δεν μπορεί να αποποιηθεί (να αρνηθεί) την υποβολή της υπογραφής του (**μη αποποίηση**).

5. Ο χρόνος υποβολής της προηγμένης ηλεκτρονικής υπογραφής (**χρονοσήμανση**) δύναται να είναι **ασφαλής**, με την έννοια ότι δεν λαμβάνεται από τον Η/Υ του υπογράφοντος, αλλά από Η/Υ του Παρόχου Υπηρεσιών Πιστοποίησης, που λειτουργεί για να παρέχει την συγκεκριμένη υπηρεσία με

ασφάλεια.

6. Μειώνει χρόνο-κόστος των αξιόπιστων,νομικά έγκυρων και ασφαλών συναλλαγών, απλοποιεί την διαδικασία ολοκλήρωσής των (δεν απαιτείται εκτύπωση).

Σύμφωνα με το **Άρθρο 26** του κανονισμού **910-2014 ΕΚ οι απαιτήσεις για τις προηγμένες ηλεκτρονικές υπογραφές** είναι:

α) συνδέεται κατά τρόπο μοναδικό με τον υπογράφοντα
β) είναι ικανή να ταυτοποιεί τον υπογράφοντα
γ) δημιουργείται με δεδομένα δημιουργίας ηλεκτρονικής υπογραφής τα οποία ο υπογράφων μπορεί, **με υψηλό βαθμό εμπιστοσύνης, να χρησιμοποιεί υπό τον αποκλειστικό του έλεγχο**, και
δ) συνδέεται με τα δεδομένα που έχουν υπογραφεί σε σχέση με αυτήν κατά τρόπο ώστε να μπορεί να ανιχνευθεί οποιαδήποτε επακόλουθη τροποποίηση των εν λόγω δεδομένων.

Η προηγμένη ηλεκτρονική υπογραφή **δεν έχει εικόνα**, είναι μία **μη ορατή** σε εμάς αλγοριθμική ψηφιακή σύνοψη του ηλεκτρονικού κειμένου που υπογράφουμε, η οποία κρυπτογραφείται και συνδέεται με το η-έγγραφο (ή η-μήνυμα) και με το πιστοποιητικό μας **με άρρηκτο και μονοσήμαντο τρόπο**. **Η προηγμένη ηλεκτρονική υπογραφή μας δεν είναι ποτέ η ίδια**, εκτός αν αφορά το ίδιο η-έγγραφο.

Το νομικό, τεχνολογικό υπόβαθρο και θεσμικό πλαίσιο της έκδοσης Πιστοποιητικών για Εγκεκριμένη Ηλεκτρονική Υπογραφή δημιουργεί την απαιτούμενη εμπιστοσύνη για τις επαγγελματικές και κοινωνικές μας συναλλαγές **με αξιοπιστία και υψηλού βαθμού ασφάλεια**. Για να διατηρούμε το υψηλό αυτό επίπεδο θα πρέπει να συμβάλλουμε και εμείς σαν Τελικοί Χρήστες (ΤΧ) **με την προστασία της Ασφαλούς Διάταξης Δημιουργίας Υπογραφής (ΑΔΔΥ, USB token, στικάκι)**, **διατηρώντας την πάντοτε κάτω από τον αποκλειστικό μας έλεγχο**.

Το γεγονός ότι σε όλη την Ευρώπη έχει υιοθετηθεί το συγκεκριμένο θεσμικό πλαίσιο και τεχνολογικό υπόβαθρο (**Υποδομή Δημόσιου Κλειδιού**, Public Key Infrastructure) μας δηλώνει τον υψηλό βαθμό αξιοπιστίας και ασφάλειας του. Γι αυτό άλλωστε έχουμε το συνεχές φαινόμενο διαδοχικής υιοθέτησής της σε διαφορετικού τομείς του δημοσίου και ιδιωτικού τομέα, όπως :

Στην **ηλεκτρονική διακυβέρνηση** (Ν 3979/2011), για υποβολή αιτημάτων και ηλεκτρονικών εγγράφων στο δημόσιο και δημόσιο τομέα (κάθε φυσικό πρόσωπο),

Ηλεκτρονικές Συμβάσεις (άρθρο 8, ΠΔ 131/2003),

Ηλεκτρονική κατάθεση δικογράφων (δικηγόροι), ηλεκτρονική χορήγηση σχετικών πιστοποιητικών και λοιπών εγγράφων στο Ελεγκτικό Συνέδριο (ΠΔ 95/2014),

Υποβολή συμμετοχής σε **διαγωνισμούς προμηθειών δημοσίου στο Εθνικό Σύστημα Ηλεκτρονικών Δημοσίων Συμβάσεων (Ε.Σ.Η.ΔΗ.Σ.)** (Ν. 4281/2014) (**επιχειρήσεις**),

Στο προσεχές μέλλον, **διαβίβαση ηλεκτρονικά στη βάση δεδομένων του Κτηματολογίου στοιχεία και συμβόλαια** ύστερα από οποιαδήποτε μεταγραφή ακινήτου σε κτηματολογικό γραφείο ή υποθηκοφυλακείο από συμβολαιογράφους (**συμβολαιογράφοι**),

Ηλεκτρονική Τιμολόγηση (ΠΟΛ 1003 31/12/2014) (**λογιστές**),

Ηλεκτρονική Συνταγογράφηση (**γιατροί**),

Υποχρεωτική (από 1.7.2015) **αποστολή εγγράφων για δημοσίευση στο Φύλλο της Εφημερίδας της Κυβέρνησης** με χρήση τεχνολογιών πληροφορικής και επικοινωνιών και προηγμένης ηλεκτρονικής υπογραφής,

Ελληνικό Δημόσιο, από **01/01/2017,** η εσωτερική διακίνηση εγγράφων θα γίνεται **υποχρεωτικά μόνο με η-έγγραφα, υπογεγραμμένα με εγκεκριμένη ηλεκτρονική υπογραφή.**

Προστασία στην διακίνηση ηλεκτρονικών εγγράφων και η-μηνυμάτων (Email) από τον κάθε ένα μας.

Ηλεκτρονική Υπογραφή με νομική ισχύ της παραγράφου 2, άρθρου 3 του ΠΔ 150/ 2001

Το νομικό πλαίσιο και οι κανονισμοί προβλέπουν την αποδοχή υιοθέτησης **μη εγκεκριμένων ηλεκτρονικών υπογραφών** για δύο λόγους :

1) για να δώσει την δυνατότητα ανάπτυξης ανάλογων καινοτομικών τεχνολογικών εφαρμογών, και **2)** για να δώσει την δυνατότητα επιλογής εφαρμογών που ταιριάζουν καλύτερα σε συγκεκριμένες ανάγκες.

Το ΠΔ 150/ 2001 άρθρο 3 παρ. 2, ορίζει ρητά ότι αν δεν συντρέχουν οι προϋποθέσεις της παρ. 1 δεν απορρίπτεται η αποδεικτική ισχύς της ηλεκτρονικής υπογραφής σε μια νομική διαδικασία. Η αποδοχή της εξαρτάται από την βούληση των συμβαλλομένων μερών, σε μια δε νομική διαδικασία ενδεχομένως να αμφισβητηθεί (όταν δεν ισχύει η ιδιότητα της “μη αποποίησης”) και οι δικαστές θα αξιολογήσουν τους ισχυρισμούς και τις αποδείξεις των συμβαλλομένων, προκειμένου να αποφασίσουν σχετικά με την νομική ισχύ της υποβαλλόμενης υπογραφής. Είναι φανερό ότι η κρίση των δικαστών επηρεάζεται από την συχνότητα φαινομένων πλαστογραφίας-παραποίησης εγγράφων και ψηφιακών υπογραφών, όπως και των συνθηκών κάτω από τις οποίες συμβαίνουν. Η συχνή υποκλοπή μιας ψηφιακής υπογραφής ενδεχομένως θα οδηγήσει σε περιπτώσεις μη αποδοχής της.

Η εγκεκριμένη ηλεκτρονική υπογραφή έχει υψηλό βαθμό ασφάλειας (δεν αντιγράφεται) και γι αυτό έχει την ιδιότητα της μη αποποίησης (μή άρνησης) υποβολής της !

Digitally signed by EMMANOUIL MIRTZANIS
DN: o=Hellenic Public Administration Certification Services, serialNumber=ERMIS-19232454, c=GR, email=emirtz@otenet.gr, sn=MIRTZANIS, givenName=EMMANOUIL, ou=ΕΜΜΑΝΟΥΗΛ ΜΙΡΤΖΑΝΗΣ, cn=EMMANOUIL MIRTZANIS
Date: 2016.12.07 22:31:17 +02'00'