

Ταυτότητα Έργου

Online έλεγχος εγκυρότητας ψηφιακών Υπογραφών

Εφαρμογή για τον online έλεγχο εγκυρότητας ψηφιακών υπογραφών

Υπεύθυνός : Παπαδόπουλος Θοδωρής (thodoris@thodoris.net)

Digital Signature Αρχική Σχετικά Επικοινωνία

Σύρετε ένα αρχείο pdf εδώ

Σχετικά

Η εφαρμογή επιτρέπει τον έλεγχο εγκυρότητας των ψηφιακών υπογραφών που βασίζονται σε πιστοποιητικό που έχει εκδοθεί από την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου. Σύρετε ένα αρχείο pdf στο παραπάνω πλαίσιο, για να δείτε πληροφορίες σχετικά με την υπογραφή που φέρει.

[περισσότερα »](#)

Ψηφιακές Υπογραφές

Η Ψηφιακή Υπογραφή που βασίζεται σε Αναγνωρισμένο Πιστοποιητικό και δημιουργείται από Ασφαλή Διάταξη Δημιουργίας Υπογραφής επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.

[περισσότερα »](#)

Όροι Χρήσης

Η χρήση του δικτυακού τόπου συμπεριλαμβανομένης της περιήγησης ιστού καθώς και σποικινδής άλλων υπηρεσιών παρέχονται από το διαδικτυακό τόπο, προϋποθέτει την ανεπιφύλακτη αποδοχή των περιγραφόμενων όρων χρήσης και συνιστά έμπρακτη αποδοχή τους.

[περισσότερα »](#)

Υλοποιήθηκε στα πλαίσια του έργου Ηλεκτρονικές Υπηρεσίες για την Ανάπτυξη και Διάδοση του Ανοιχτού Λογισμικού

ΠΕΡΙΓΡΑΦΗ

Η εφαρμογή **Online έλεγχος εγκυρότητας ψηφιακών Υπογραφών**

(DigitalSignatureCheckGR) επιτρέπει τον έλεγχο εγκυρότητας των ψηφιακών υπογραφών που βασίζονται σε πιστοποιητικό που έχει εκδοθεί από την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου. Η τελευταία έκδοση της εφαρμογής φιλοξενείται στην ιστοσελίδα : digitalsignature.gr

Η εφαρμογή έχει αναπτυχθεί στα πλαίσια του έργου "Ηλεκτρονικές Υπηρεσίες για την ανάπτυξη και διάδοση του Ανοιχτού Λογισμικού"

ΔΥΝΗΤΙΚΟΙ ΧΡΗΣΤΕΣ

Η εφαρμογή προβλέπεται να εξυπηρετήσει ιδιαίτερα :

- **Υπαλλήλους φορέων του Δημοσίου** , οι οποίοι καλούνται να εξυπηρετήσουν αιτήματα πολιτών που έχουν σταλεί με χρήση ψηφιακά υπογεγραμμένων αρχείων.
- **Εταιρίες και Νομικά πρόσωπα** που θέλουν να συμμετάσχουν σε ηλεκτρονικούς διαγωνισμούς μέσω της πλατφόρμας ηλεκτρονικών προμηθειών , και θέλουν να ελέγχουν αν τα ηλεκτρονικά δικαιολογητικά που υποβάλλουν φέρουν έγκυρη ηλεκτρονική υπογραφή.
- **Δικηγόρους και Συμβολαιογράφους** , που χρησιμοποιούν ηλεκτρονικές υπογραφές για την κατάθεση δικογράφων και την ηλεκτρονική διαβίβαση στοιχείων και αντιγράφων συμβολαιογραφικών πράξεων.
- **Τράπεζες και άλλα Ιδρύματα** που καλούνται συχνά να ελέγχουν τα πιστοποιητικά εταιριών από το ΓΕΜΗ ή άλλα έγγραφα πελατών τους που κατατίθενται ηλεκτρονικά.

ΑΝΑΜΕΝΩΜΕΝΑ ΩΦΕΛΗ

Με το Π.Δ 150/2001 ενσωματώθηκε στο ελληνικό δίκαιο η Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές». Σύμφωνα με αυτό, μία ηλεκτρονική υπογραφή (δηλαδή δεδομένα σε ηλεκτρονική μορφή συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετιζόμενα λογικά με αυτά που χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας) επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο, εφόσον πληροί τις ουσιαστικές και τυπικές προϋποθέσεις που προβλέπονται. Αυτό σημαίνει ότι υπό συγκεκριμένες προϋποθέσεις, τα πρόσωπα που συμβάλλονται σε μία ηλεκτρονική συναλλαγή, και υπογράφουν ηλεκτρονικά, δεν μπορεί να την αρνηθούν. Επιπλέον κάθε πρόσωπο (φυσικό ή νομικό , ιδιωτικό ή δημόσιο) δεν μπορεί να μην κάνει δεκτό έγγραφο το οποίο έχει σταλεί ηλεκτρονικά και φέρει έγκυρη ηλεκτρονική υπογραφή.

Ένας από τους σημαντικότερους , μέχρι σήμερα , ανασταλτικούς παράγοντες για την διάχυση της χρήσης ψηφιακών υπογραφών είναι ο υψηλός βαθμός τεχνογνωσίας που απαιτείται από την πλευρά του παραλήπτη προκειμένου να μπορέσει να προβεί σε έλεγχο εγκυρότητας μιας ηλεκτρονικής υπογραφής. Ενδεικτικά αναφέρεται ότι απαιτείται η εγκατάσταση πρωτευουσών και υποκείμενων αρχών πιστοποίησης στο Certificate Store του υπολογιστή , η ρύθμιση των εξυπηρετητών χρονοσήμανσης και η παραμετροποίηση των επιμέρους προγραμμάτων (π.χ Acrobat Reader). Τα παραπάνω πρέπει να γίνουν σε όλους τους υπολογιστές του χρήστη με διαφορετικά βήματα ανάλογα με τον τύπο και το λειτουργικό του υπολογιστή. Επιπλέον ο έλεγχος εγκυρότητας σε φορητές συσκευές είναι ανάλογα με τον τύπο της συσκευής , από ιδιαίτερα δύσκολος έως και αδύνατος.

Το σύστημα που αναπτύχθηκε θα διευκολύνει σημαντικά την διαδικασία ελέγχου της εγκυρότητας ψηφιακά υπογεγραμμένων εγγράφων , καθώς τα βήματα που

απαιτούνται για να πραγματοποιηθεί ο έλεγχος περιορίζονται σημαντικά. Ο χρήστης επισκέπτεται τον δικτυακό τόπο που φιλοξενεί το σύστημα και κάνοντας Upload (με δυνατότητα drag & drop) ένα αρχείο παίρνει απάντηση σε φυσική γλώσσα σχετικά με την εγκυρότητα της υπογραφής και στοιχεία σχετικά με τον υπογράφο του εγγράφου.

ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

Η εφαρμογή συνοδεύεται από έναν δικτυακό τόπο στον οποίο μπορεί ο καθένας να υποβάλει ένα ψηφιακά υπογεγραμμένο έγγραφο και σε πραγματικό χρόνο να δει όλες τις ψηφιακές υπογραφές που περιέχει καθώς και αν αυτές θεωρούνται έγκυρες με βάση το ισχύον θεσμικό πλαίσιο (σύμφωνα με τα οριζόμενα στο Π.Δ. 150/2001).

Το σύστημα κάνει χρήση βιβλιοθηκών ανοιχτού λογισμικού (iText & Bouncy Castle) για να αναλύσει όλες τις ψηφιακές υπογραφές ενός εγγράφου. Προκειμένου να αποφανθεί εάν μια υπογραφή είναι έγκυρη το σύστημα εκτελεί συνδυαστικά τους παρακάτω ελέγχους :

- Έλεγχος εάν η υπογραφή βασίζεται σε αναγνωρισμένο πιστοποιητικό.
- Έλεγχος εάν η υπογραφή έχει ενσωματωμένη χρονοσήμανση
- Έλεγχος ότι το πιστοποιητικό δεν έχει ανακληθεί (CRL - certificate revocation list).
- Έλεγχος ότι το υπογεγραμμένο έγγραφο δεν έχει τροποποιηθεί , από την στιγμή της υπογραφής του.

Τα αποτελέσματα σχετικά με την εγκυρότητα της ψηφιακής υπογραφής εμφανίζονται στον χρήστη σε φυσική γλώσσα , επιτρέποντας του να κατανοήσει άμεσα και εύκολα την εγκυρότητα της υπογραφής.

Στην αρχική σελίδα ο χρήστης καλείται να ανεβάσει (με δυνατότητα Drag & drop) ένα ψηφιακά υπογεγραμμένο PDF αρχείο. Μετά την επιτυχή μεταφόρτωση του αρχείου η εφαρμογή αναλύει τις ψηφιακές υπογραφές και παρουσιάζει λεπτομέρειες για κάθε μια υπογραφή που εντοπίστηκε στο έγγραφο.

Στις λεπτομέρειες κάθε υπογραφής περιλαμβάνονται:

- Ημερομηνία Υπογραφής
- Χρονοσήμανση
- Αλγόριθμος Σύνοψης
- Ακεραιότητα εγγράφου
- Εγκυρότητα την Ημ.Υπογραφής
- Εγκυρότητα Τώρα
- Ορατή Υπογραφή
- Τοποθεσία
- Σκοπός

Ενώ για κάθε ψηφιακό πιστοποιητικό εμφανίζονται πληροφορίες για :

- Εκδότης
- Θέμα
- Έγκυρο από
- Έγκυρο Έως
- Σκληρής Αποθήκευσης
- Εγκυρότητα την Ημ.Υπογραφής
- Εγκυρότητα Τώρα

ΤΕΧΝΟΛΟΓΙΕΣ

Το έργο έχει αναπτυχθεί σε ASP.NET MVC 5 και χρησιμοποιεί τις βιβλιοθήκες ανοιχτού κώδικα :

- iTextSharp (Pdf Handling)
- JQuery (js utils)
- handlebars.js (templating)
- DropZone (File Uploads)
- bootstrap (UI)

ΑΠΟΘΕΤΗΡΙΟ ΤΟΥ ΕΡΓΟΥ

Το έργο διατίθεται με ανοικτή άδεια EUPL v1.1(<http://ec.europa.eu/idabc/eupl.html>) και ο κώδικας είναι διαθέσιμος μέσω του αποθετηρίου <https://github.com/ellak-monades-aristeias/DigitalSignatureCheckGR>

ΠΑΡΑΔΟΤΕΑ

Τα τελικά παραδοτέα του έργου αποτελούνται από :

- Τον δικτυακό τόπο σε δικό του domain , στον οποίο φιλοξενείται σε πλήρη λειτουργία το περιγραφόμενο σύστημα.
- Το σύνολο κώδικα σε αποθετήριο github
- Την τεχνική τεκμηρίωση του συστήματος.

Πίνακας παραδοτέων

A/ A	Περιγραφή δράσης	Τεκμηρίωση
A	Έκδοση 1.0 της εφαρμογής	Η εφαρμογή υπάρχει διαθέσιμη σε αυτόν τον σύνδεσμο: http://www.digitalsignature.gr
B	Υλικό για διασφάλιση της δυνατότητας διάχυσης της εφαρμογής	
B1	Προσφορά του κώδικα της εφαρμογής ως ανοικτού κώδικα.	Το έργο βρίσκεται στο GitHub σε αυτόν τον σύνδεσμο: https://github.com/ellak-monades-aristeias/DigitalSignatureCheckGR
B2	Υποστηρικτικό υλικό (τεκμηρίωση, εγχειρίδιο κ.λπ.)	Η τεκμηρίωση είναι στο GitHub.
Γ	Πρωώθηση	
Γ1	Αποστολή ενημερωτικού email	Έχει αποσταλεί ενημερωτικό email προς την ΑΠΕΔ (Αρχή Πιστοποίησης του Ελληνικού Δημοσίου) σχετικά με τον δικτυακό τόπο digitalsignature.gr
Γ2	Πρωώθηση στα social media	<ul style="list-style-type: none">• Google+ (https://plus.google.com/u/0/105000871986808437922)• Twitter (https://twitter.com/thodoris)