Ζευς—Οδηγίες Διαχείρισης Ψηφοφορίας

Ομάδα Ανάπτυξης Συστήματος Ζευς

18 Οκτωβρίου 2012

Το παρόν κείμενο περιγράφει τη διαχείριση ψηφιακών ψηφοφοριών μέσω του συστήματος Ζευς. Απευθύνεται καταρχήν στον διαχειριστή της εκάστοτε ψηφοφορίας και στα μέλη της εφορευτικής επιτροπής. Εντούτοις, και οι ψηφοφόροι μπορεί να βρουν ενδιαφέρουσα την περιγραφή των λειτουργιών για μια καλύτερη κατανόηση της διαδικασίας.

Το σύστημα Ζευς είναι μία υλοποίηση εκλογών αποκλειστικά με ψηφιακά μέσα. Τόσο η προετοιμασία της ψηφοφορίας, όσο και η ψηφοφορία αυτή καθ' αυτή γίνονται μέσω υπολογιστή. Τα ψηφοδέλτια είναι ψηφιακά, και η διαδικασία καταμέτρησης γίνεται μέσω κρυπτογραφικών αλγορίθμων που εγγυώνται τόσο την ανωνυμία του χρήστη όσο και την εξασφάλιση ότι όλα τα ψηφοδέλτια καταμετρώνται σωστά.

Η Διαδικασία Επιγραμματικά

Μία ψηφοφορία με το σύστημα Ζευς περιλαμβάνει τα παρακάτω βήματα:

1. Η διεξάγουσα αρχή συντάσσει τα ψηφοδέλτια και τη λίστα των ψηφοφόρων και ορίζει την εφορευτική επιτροπή. Η λίστα των ψηφοφόρων αποτελείται από τα ονοματεπώνυμά τους και την ηλεκτρονική τους διεύθυνση.
2. Οι ψηφοφόροι λαμβάνουν στην ηλεκτρονική τους διεύθυνση μήνυμα με το οποίο καλούνται να ψηφίσουν. Το μήνυμα περιέχει σύνδεσμο (link) που οδηγεί στο ψηφιακό παραπέτασμα μέσα στο οποίο προετοιμάζεται η ψήφος. Το παραπέτασμα θα ενεργοποιηθεί όταν η εφορευτική επιτροπή εκκινήσει την ψηφοφορία[1].
3. Η εφορευτική επιτροπή δίνει τους χρόνους έναρξης και λήξης της ψηφοφορίας.
4. Οι ψηφοφόροι ψηφίζουν εντός του ορισμένου χρονικού διαστήματος, και λαμβάνουν ψηφιακή απόδειξη της συμμετοχής τους.
5. Με το πέρας της ψηφοφορίας, η εφορευτική επιτροπή δίνει την εντολή για την αυτόματη κατάμετρηση των ψηφοδελτίων.

[1] Συνεπώς για κάθε ψηφοφόρο το παραπέτασμα είναι μια εξατομικευμένη σελίδα στον Παγκόσμιο Ιστό, όπου αυτός μπορεί να υποβάλλει την ψήφο του.

Η επικοινωνία των αρχών και των ψηφοφόρων με το πληροφοριακό σύστημα Ζευς γίνεται μέσω ενός απλού προγράμματος περιήγησης του Παγκόσμιου Ιστού (web browser), ενώ προστατεύεται όπως ακριβώς και οι οικονομικές συναλλαγές μέσω Διαδικτύου. Η ακεραιότητα της ψηφοφορίας είναι μαθηματικά επαληθεύσιμη από τον καθένα μέσω της χρήσης κρυπτογραφίας, και χωρίς καμία προσβολή του

απόρρητου. Το απόρρητο της ψήφου είναι ευθύνη της εφορευτικής επιτροπής, και είναι πρακτικά εξασφαλισμένο καθώς μπορεί να παραβιαστεί μόνο με συνεννόηση όλων των μελών της εφορευτικής επιτροπής και του διαχειριστή του συστήματος Ζευς.

Προετοιμασία της Ψηφοφορίας

Η προετοιμασία της ψηφοφορίας περιλαμβάνει τον ορισμό της εφορευτικής επιτροπής στο σύστημα, την εισαγωγή των ψηφοφόρων και μερικών επιπλέον παραμέτρων. Στην προετοιμασία της ψηψοφορίας συμμετέχουν ο διαχειριστής της ψηφοφορίας και η εφορευτική επιτροπή[2].

[2] Ο διαχειριστής της ψηφοφορίας είναι ένας χρήστης του συστήματος Ζευς. Δεν είναι ο διαχειριστής του ίδιου του συστήματος Ζευς. Διαχειριστής του συστήματος Ζευς είναι η ομάδα που είναι επιφορτισμένη με τη σωστή εγκατάσταση και λειτουργία του.

Εισαγωγή Παραμέτρων Ψηφοφορίας

Ο διαχειριστής της ψηφοφορίας μπαίνει στο σύστημα Ζευς δίνοντας τους κωδικούς πρόσβασης που του έχουν παραδοθεί. Αυτός εισάγει στο σύστημα τις βασικές παραμέτρους της ψηφοφορίας. Μπορεί να είναι μέλος της εφορευτικής επιτροπής[3]. Οι βασικές παράμετροι της ψηφοφορίας είναι:

[3] Σε κάθε περίπτωση καλό είναι ο διαχειριστής της ψηφοφορίας να είναι εξοικειωμένος με τεχνολογίες πληροφορικής, αν και δεν απαιτείται να είναι επαγγελματίας του χώρου.

Τίτλος Ένας επιγραμματικός τίτλος για την ψηφοφορία.

Περιγραφή Μία πιο αναλυτική περιγραφή.

Χρόνος έναρξης Ημερομηνία και ώρα που θα μπορούν οι ψηφοφόροι να ξεκινήσουν να ψηφίζουν.

Χρόνος λήξης Ημερομηνία και ώρα όπου οι ψηφοφόροι δεν θα μπορούν πλέον να ψηφίσουν και θα μπορεί να ξεκινήσει η καταμέτρηση.[4]

[4] Αν χρειαστεί ο χρόνος λήξης μπορεί να παραταθεί.

Μέλη της εφορευτικής επιτροπής Ονοματεπώνυμο και διεύθυνση ηλεκτρονικού ταχυδρομείου κάθε μέλους, μία γραμμή για κάθε μέλος.

Σχολές και ανεξάρτητα τμήματα Είναι απαραίτητο για τον κανόνα των “2” που θα δούμε παρακάτω.

Πλήθος εκλεγόμενων Σύμφωνα με το νόμο μπορεί να είναι 6 ή 8.

Κανόνας των “2” Περιορισμός εκλογής 2 υποψηφίων ανά σχολή ή ανεξάρτητο τμήμα.

Στοιχεία επικοινωνίας Τηλέφωνο και ηλεκτρονικό ταχυδρομείο της εφορευτικής επιτροπής, θα εμφανίζεται στην επικοινωνία με τους ψηφοφόρους.

Αποστολή Μηνυμάτων στα Μέλη της Εφορευτικής Επιτροπής

Όταν εισαχθούν οι παράμετροι της ψηφοφορίας, ο Ζευς θα στείλει στα μέλη της εφορευτικής επιτροπής ηλεκτρονικό μήνυμα όπως το παρακάτω[5]:

[5] Το θέμα (subject) του μηνύματος περιέχει τον αριθμό 1, τα μέλη της εφορευτικής επιτροπής θα λάβουν και άλλο μήνυμα στη συνέχεια.

```
Προεδρικές εκλογές ΗΠΑ Νοεμβρίου 2012: παρακαλούμε για τις ενέργειές σας, #1

Ως μέλος της εφορευτικής επιτροπής της ψηφοφορίας

    Προεδρικές εκλογές ΗΠΑ Νοεμβρίου 2012

  παρακαλούμε επισκεφθείτε τον πίνακα ελέγχου και ακολουθήστε τις οδηγίες

    https://zeus.minedu.gov.gr/helios/t/2012-10-18-1/louridas@grnet.gr/ASD0m24OmdOC

  --
  Ψηφιακή Κάλπη «Ζευς»
```

Μέσω του συνδέσμου που δίνεται στο ηλεκτρονικό μήνυμα ο παραλήπτης μπορεί να προχωρήσει στην παραγωγή του προσωπικού του Κωδικού Ψηφοφορίας.

Παραγωγή Κωδικών Ψηφοφορίας

Κάθε μέλος της εφορευτικής επιτροπής δημιουργεί και κρατάει στην κατοχή του έναν Κωδικό Ψηφοφορίας. Ο Κωδικός Ψηφοφορίας αποτελείται από ένα δημόσιο και ένα ιδιωτικό μέρος. Το ιδιωτικό μέρος, το οποίο δεν θα πρέπει να διαρρεύσει, θα χρησιμοποιηθεί για την αποκρυπτογράφηση και καταμέτρηση των ψηφοδελτίων.

Ο Κωδικός Ψηφοφορίας παράγεται τοπικά στον τοπικό υπολογιστή του μέλους της εφορευτικής επιτροπής[6]. Αυτό γίνεται ακολουθώντας τις οδηγίες στη σελίδα που του υποδεικνύεται στο μήνυμα που έλαβε το μέλος της εφορευτικής επιτροπής.

[6] Η παραγωγή γίνεται στο πρόγραμμα περιήγησης του χρήστη με τη χρήση γλώσσας Javascript.

Αφού παραχθεί ο Κωδικός, το μέλος της εφορευτικής επιτροπής θα πρέπει να τον αποθηκεύσει σε ασφαλές μέρος. Σε περίπτωση που χαθεί, δεν θα είναι δυνατή η αποκρυπτογράφηση των ψηφοδελτίων και η καταμέτρησή τους[7].

[7] Αν θέλετε να δείτε πώς είναι ένας κωδικός ψηφοφορίας, πηγαίνετε στη σελίδα **??**.

Καθώς ο Κωδικός έχει δημιουργηθεί στον τοπικό υπολογιστή του μέλους της εφορευτικής επιτροπής, ο Ζευς ακόμα δεν γνωρίζει τίποτε για αυτόν. Για να ενημερωθεί το σύστημα για την ύπαρξη του Κωδικού, το μέλος της εφορευτικής επιτροπής πρέπει να προχωρήσει στην ενεργοποίηση του Κωδικού. Με την ενεργοποίηση του Κωδικού αποστέλλεται στο σύστημα το δημόσιο *και μόνο* μέρος του Κωδικού.

Μετά την επιτυχή ενεργοποίηση, το μέλος της εφορευτικής επιτροπής αποσυνδέεται από το σύστημα. Αυτό γίνεται ώστε να είμαστε σίγουροι ότι στο επόμενο βήμα, την επαλήθευση του κωδικού, το μέλος της επιτροπής πραγματικά μπορεί να εντοπίσει το αποθηκευμένο αρχείο με τον Κωδικό του.

Στη συνέχεια το μέλος της εφορευτικής επιτροπής πρέπει να επαληθεύσει την κατοχή του Κωδικού του στο σύστημα. Ο Ζευς ενημερώνει το μέλος της εφορευτικής επιτροπής με μήνυμα της μορφής[8]:

[8] Το θέμα (subject) του μηνύματος περιέχει τον αριθμό 2, είναι το δεύτερο μήνυμα που λαμβάνει το μέλος της επιτροπής.

```
Προεδρικές εκλογές ΗΠΑ Νοεμβρίου 2012: παρακαλούμε για τις ενέργειές σας, #2

Ως μέλος της εφορευτικής επιτροπής της ψηφοφορίας

    Προεδρικές εκλογές ΗΠΑ Νοεμβρίου 2012

  παρακαλούμε επισκεφθείτε τον πίνακα ελέγχου και ακολουθήστε τις οδηγίες

    https://zeus.minedu.gov.gr/helios/t/2012-10-18-1/voter@foo.bar/WUT
0q34OadOC

  --
  Ψηφιακή Κάλπη «Ζευς»
```

Πατώντας στο σύνδεσμο του μηνύματος θα εμφανιστεί οθόνη στην οποία το μέλος της εφορευτικής επιτροπής θα επαληθεύσει την κατοχή του Κωδικού του. Αυτό το κάνει επιλέγοντας το αρχείο με τον Κωδικό του, και ζητώντας να ελεγχθεί από το σύστημα. Το σύστημα θα ελέγξει ότι πράγματι τα δημόσια μέρη του Κωδικού ταυτίζονται.

Προσθήκη Υποψηφίων

Η εισαγωγή των υποψηφίων στο σύστημα είναι ευθύνη του διαχειριστή. Ο διαχειριστής τους εισάγει μέσω κατάλληλης φόρμας, δίνοντας για κάθε έναν από αυτούς:

- όνομα
- επώνυμο
- πατρώνυμο
- σχολή

Προσθήκη Ψηφοφόρων

Η εσαγωγή των ψηφοφόρων στο σύστημα γίνεται και αυτή από τον διαχειριστή. Ο διαχειριστής θα πρέπει να μεταφορτώσει (upload) αρχείο μορφής CSV[9] στο σύστημα. Το αρχείο αυτό θα πρέπει να αποτελείται από γραμμές της μορφής:

[9] Comma Separated Values, `http://en.wikipedia.org/wiki/Comma-separated_values`.

```
myname@foo.bar,Όνομα,Επώνυμο,Πατρώνυμο
```

όπου το πεδίο Πατρώνυμο είναι προαιρετικό. Μετά τη μεταφόρτωση του αρχείου, και αφού αυτό ελεγθχεί από το σύστημα, η λίστα των ψηφοφόρων εμφανίζεται στην οθόνη του διαχειριστή για έναν επιπλέον έλεγχο.

Για την παραγωγή του απαιτούμενου αρχείου CSV μπορεί να χρησιμοποιηθεί ένα πρόγραμμα λογιστικών φύλλων (π.χ. MS-Excel ή LibreOffice Spreadsheet). Το λογιστικό φύλλο θα πρέπει να έχει τρεις ή τέσσερεις στήλες που να αντιστοιχούν στη διεύθυνση ηλεκτρονικού ταχυδρομείου, όνομα, επώνυμο και προαιρετικά το πατρώνυμο του υποψηφίου, και να μην έχει επικεφαλλίδες ή άλλα περιττά στοιχεία. Θα πρέπει να δοθεί προσοχή κατά την εξαγωγή του αρχείου CSV ώστε ο χαρακτήρας διαχωρισμού των πεδίων να είναι το κόμμα, και τα ελληνικά να έχουν κωδικοποιηθεί σωστά. Ο καλύτερος τρόπος να επιβεβαιωθεί αυτό είναι να ανοιχτεί το αρχείο μέσω ενός προγράμματος διόρθωσης κειμένου (text editor), όπως το Notepad ή το TextEdit[10].

[10] Ή ο emacs ή ο vim.

Οριστικοποίηση Ψηφοφορίας

Η προετοιμασία της ψηφοφορίας ολοκληρώνεται με την *οριστικοποίησή* της, κατά την οποία ο διαχειριστής επιβεβαιώνει ότι όλα τα στοιχεία είναι ορθά. Η οριστικοποίηση μπορεί να γίνει μόνο αν έχουν γίνει όλα τα προηγούμενα βήματα, δηλαδή:

- έχουν δημιουργηθεί όλοι οι Κωδικοί Ψηφοφορίας για τα μέλη της εφορευτικής επιτροπής
- έχουν επιβεβαιωθεί όλοι οι Κωδικοί Ψηφοφορίας από τα μέλη της εφορευτικής επιτροπής
- έχουν εισαχθεί οι υποψήφιοι
- έχουν εισαχθεί οι ψηφοφόροι

Με την ολοκλήρωση της ψηφοφορίας αποστέλλονται ηλεκτρονικά μηνύματα στους ψηφοφόρους, με τα οποία καλούνται να ψηφίσουν. Τα μηνύματα είναι της μορφής:

```
Νόμιμος παραλήπτης: Λουρίδας Παναγιώτης
```

Αξιότιμε/η κ. εκλέκτορα,

Καλείστε να συμμετάσχετε στην ψηφοφορία

  Προεδρικές Εκλογές ΗΠΑ Νοέμβριος 2012

που αρχίζει στις Oct. 18, 2012, 11 π.μ.
και λήγει στις Oct. 18, 2012, 11 μ.μ.

Υποβάλετε την ψήφο σας, ακολουθώντας το σύνδεσμο

https://zeus.minedu.gov.gr/helios/elections/4ec48876-19
00-11e2-aaa8-aa000039f982/l/a5319ab0-350f-4231-baf5-58f
965df444c/HdkrIk60RH

Ενημερωτικά:

* Για πληροφορίες σχετικά με τη διαδικασία των εκλογών μπορείτε να
  επικοινωνείτε με την εφορευτική επιτροπή, τηλεφωνικώς

    3066 69999999

  ή μέσω ηλεκτρονικού ταχυδρομείου στη διεύθυνση

    someone@foo.bar

* Εάν βρίσκεστε σε διαδικασία υποβολής ψήφου ελέγχου,
  οι έγκυροι κωδικοί ελέγχου είναι οι
  ZpO5d ct3S3 9uc5e 8sF8c
  σε άλλη περίπτωση αγνοήστε τους.

Προσοχή:
Το παρόν μήνυμα είναι αυστηρώς προσωπικό και εξατομικευμένο.
Δεν επιτρεπεται η προώθηση και η επίδειξή του σε τρίτους.
Εάν δεν είστε ο νόμιμος παραλήπτης, παρακαλούμε να το
διαγράψετε αμέσως και να επικοινωνήσετε στην ηλεκτρονική διεύθυνση
helpdesk@zeus.grnet.gr

--
Ψηφιακή κάλπη «Ζευς»

Η οριστικοποίηση της ψηφοφορίας και η αποστολή των μηνυμάτων δεν είναι ανάγκη να γίνουν την τελευταία στιγμή πριν την έναρξη της διαδικασίας. Αντιθέτως, καλό είναι να γίνουν τουλάχιστον την προηγούμενη ημέρα ώστε οι ψηφοφόροι να έχουν χρόνο να δουν και να διαβάσουν τα μηνύματά τους (εξάλλου η παράδοση ενός ηλεκτρονικού μηνύματος δεν είναι πάντα στιγμιαία, και δεν εξαρτάται από το σύστημα Ζευς).

Η Σειρά των Ψηφοφόρων

Μετά την οριστικοποίηση της ψηφοφορίας, ο κάθε ψηφορόρος θα λάβει ένα μήνυμα όπως αυτό που περιγράφηκε παραπάνω. Θα πρέπει να ψηφίσει μέσα στα χρονικά όρια που περιγράφονται—την έναρξη και τη λήξη της ψηφοφορίας. Αν επισκεφθεί τον προσωπικό του σύνδεσμο για την ψηφοφορία πριν την έναρξή της, θα ενημερωθεί για την ακριβή ημερομηνία και ώρα έναρξης, χωρίς να μπορεί να καταθέσει την ψήφο του. Αν έχει ξεκινήσει η ψηφοφορία θα μπορέσει κανονικά να καταθέσει την ψήφο του.

Παράδειγμα Κωδικού Ψηφοφορίας

Ο Κωδικός Ψηφοφορίας είναι ένα αρχείο της παρακάτω μορφής:


```
{”public_key”:
  {”g”:
    ”191670661870220474364784133728808243134386787978871700309483647086956234540025828209389329618032610222778298532142870637575898198071166776505669965855352086495404484321968064549481329460133297651418835583676535986795711992517741199764492051712626369380960655352991036388904297177136464074833201090712526539167303862043809968274491783890449424280786699479381632526157513452930144493178834329005040746268732157176616483562814472745081246436392023683689710234896276325462772016619213954426436261915321128737631597220624065628074400868835360467201119220749215283408030815813952731350504229677879118796838413942889350137513”,
  ”p”:
”199362167785662787690002537031818215307777245138869842974722780952776364560876909558689003097388724192175963175258914981284240733958400605138949623375982643225580552305667862687145027380129166695179127198603098190862618170939990474261056458280975626359120237670884106841536156899140529356986274626937727835086818069064527331531161192221819112809903977527285291378947093116597304476230905004593401556539686088955724261467880214096575027803991506253627710730128611370051343553053978372083059218031533080695911848641768762795509628312732525638659045052391637779346487255903260755803947126449729259073148170769908004691077”,
  ”q”:
”996810838928313938450012685159091076538886225694349214873613904763881822804384
```

54779344501548694362096087981587629457490642120366979200302569474811687991321612790276152833931343572513690064583347589563599301549095431309085469995237130528229140487813179560118835442053420768078449570264678493137313468863917543409034532263665765580596110909556404951988763642645689473546558298652238115452502296700778269843044477862130733940107048287513901995753126813855365064305685025671776526989186041529609015766540347955924320884381397754814156366262819329522526195818889673243627951630377901973563224864629536574085384954002345533”,
”y”:
”18355687693990767971369655479132378514616095113837884021043170686761540852449513559091817824261376106430550760002503587528939343914958576007846799970703342603697984363556688224320735578625506899828422215506843320256221689910848754470396467592655294299035004425832394617387765214836641176284143146404174106960099773329109679072255364052680150167521474615017662346454385678221501887006440236943762201253680793509073584513204817817118122197680352856671577593022259487049596052689105524570901595026640787063406549590883080585408294430770072478261502958884140076526080831534156388922850002808451952638229116586190473614987”},
”x”:
”74060407269684774388402894849342662687632161895067162124533617041934012598036437850253886236492200766148034364603043273330834495596115357455751553340842840993304962525739786932652931277188499975650474425990580422699114010554544541416019444542335961903123305404423016289456634378538679945809513581407054743953245169589694209127142051499972946921333799154152465681323977716097488857383581506923864937420020678687956960032050434014815547779639488703382219472692418965649559869256671434073992091798358712556842900678127187418078921977075976155086924928807111902620968627572591528615937533472182490816989240925467}

Εννοείται ότι δεν πρέπει να αλλαχθεί από το μέλος της εφορευτικής επιτροπής.