

Zeus—Οδηγίες Διαχείρισης Ψηφοφορίας

Ομάδα Ανάπτυξης Συστήματος Zeus

18 Οκτωβρίου 2012

Το παρόν κείμενο περιγράφει τη διαχείριση ψηφιακών ψηφοφοριών μέσω του συστήματος Zeus. 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 Zeus 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 Επιγραμματα

Μία ψηφοφορία με το σύστημα Zeus 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 ψηφοφορία¹.
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 Zeus 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 Zeus.

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 ψηφοφορίας συμμετέχουν ο διαχειριστής της ψηφοφορίας και η εφορευτική επιτροπή².

Εισαγωγή Παραμέτρων Ψηφοφορίας

Ο διαχειριστής της ψηφοφορίας μπαίνει στο σύστημα Zeus δίνοντας τους κωδικούς πρόσβασης που του έχουν παραδοθεί. Αυτός εισάγει στο σύστημα τις βασικές παραμέτρους της ψηφοφορίας. Μπορεί να είναι μέλος της εφορευτικής επιτροπής³. Οι βασικές παράμετροι της ψηφοφορίας είναι:

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

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 Zeus θα στείλει στα μέλη της εφορευτικής επιτροπής ηλεκτρονικό μήνυμα όπως το παρακάτω⁵:

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

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.

⁴ Αν χρειαστεί ο χρόνος λήξης μπορεί να παραταθεί.

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

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/ASD0m240md0C>

--

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 επιτροπής⁶. Αυτό γίνεται ακολουθώντας τις οδηγίες στη σελίδα που του υποδεικνύεται στο μήνυμα που έλαβε το μέλος της εφορευτικής επιτροπής.

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 τους⁷.

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 μορφής⁸:

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

⁷ Αν θέλετε να δείτε πώς είναι ένας κωδικός ψηφοφορίας, πηγαίνετε στη σελίδα 7.

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/WUT0q340ad0C>

--

Ψηφιακή Κάλπη «Ζεϋς»

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 εισαγωγή των ψηφοφόρων στο σύστημα γίνεται και αυτή από τον διαχειριστή. Ο διαχειριστής θα πρέπει να μεταφορτώσει (upload) αρχείο μορφής CSV⁹ στο σύστημα. Το αρχείο αυτό θα πρέπει να αποτελείται από γραμμές της μορφής:

myname@foo.bar, Όνομα, Επώνυμο, Πατρώνυμο

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

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

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 τέσσερις στήλες που να αντιστοιχούν στη διεύθυνση ηλεκτρονικού ταχυδρομείου, όνομα, επώνυμο και προαιρετικά το πατρώνυμο του υποψηφίου, και να μην έχει επικεφαλίδες 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 TextEdit¹⁰.

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/4ec48876-1900-11e2-aaa8-aa000039f982/1/a5319ab0-350f-4231-baf5-58f965df444c/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
Zp05d ct3S3 9uc5e 8sF8c
σε άλλη περίπτωση αγνοήστε τους.

Προσοχή:

Το παρόν μήνυμα είναι αυστηρώς προσωπικό και εξατομικευμένο.

Δεν επιτρέπεται 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 κάλη «Zeus»

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 Zeus).

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”:

”19167066187022047436478413372880824313438678797887170030948364708695623454
0025828209389329618032610222778298532142870637575898198071166776505669965855352
0864954044843219680645494813294601332976514188355836765359867957119925177411997
6449205171262636938096065535299103638890429717713646407483320109071252653916730
3862043809968274491783890449424280786699479381632526157513452930144493178834329
0050407462687321571766164835628144727450812464363920236836897102348962763254627
7201661921395442643626191532112873763159722062406562807440086883536046720111922
074921528340803081581395273135050422967787911879683841394288935013751”,

”p”:

”199362167785662787690002537031818215307777245138869842974722780952776364560876
9095586890030973887241921759631752589149812842407339584006051389496233759826432
2558055230566786268714502738012916669517912719860309819086261817093999047426105
6458280975626359120237670884106841536156899140529356986274626937727835086818069
0645273315311611922218191128099039775272852913789470931165973044762309050045934
0155653968608895572426146788021409657502780399150625362771073012861137005134355
3053978372083059218031533080695911848641768762795509628312732525638659045052391
63777934648725590326075580394712644972925907314817076990800469107”,

”q”:

”996810838928313938450012685159091076538886225694349214873613904763881822804384
5477934450154869436209608798158762945749064212036697920030256947481168799132161
2790276152833931343572513690064583347589563599301549095431309085469995237130528
2291404878131795601188354420534207680784495702646784931373134688639175434090345
3226366576558059611090955640495198876364264568947354655829865223811545250229670
0778269843044477862130733940107048287513901995753126813855365064305685025671776
5269891860415296090157665403479559243208843813977548141563662628193295225261958
1888967324362795163037790197356322486462953657408538495400234553”,

”y”:

”183556876939907679713696554791323785146160951138378840210431706867615408524495
1355909181782426137610643055076000250358752893934391495857600784679997070334260
3697984363556688224320735578625506899828422215506843320256221689910848754470396
4675926552942990350044258323946173877652148366411762841431464041741069600997733
2910967907225536405268015016752147461501766234645438567822150188700644023694376
2201253680793509073584513204817817118122197680352856671577593022259487049596052
6891055245709015950266407870634065495908830805854082944307700724782615029588841
40076526080831534156388922850002808451952638229116586190473614987”,

”x”:



”740604072696847743884028948493426626876321618950671621245336170419340125980364
3785025388623649220076614803436460304327333083449559611535745575155334084284099
3304962525739786932652931277188499975650474425990580422699114010554544541416019
4445423359619031233054044230162894566343785386799458095135814070547439532451695
8969420912714205149997294692133379915415246568132397771609748885738358150692386
4937420020678687956960032050434014815547779639488703382219472692418965649559869
2566714340739920917983587125568429006781271874180789219770759761550869249288071
1190262096862757259152861593753347218249081698924092546”}

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