Notă tehnică

privind utilizarea votului electronic

Platforma de vot electronic, dezvoltată de administratorul aplicației IFEP - Tabloul Național al Avocaților – Portal IFEP, are ca scop asigurarea suportului necesar pentru organizarea proiectelor de tip vot electronic.

În dezvoltarea acestui modul s-a acordat o atenție deosebită următoarelor aspecte:

- Securitatea și confidențialitatea votului electronic;
- Ușurința în exploatare;
- Trasabilitatea acțiunilor și adaptabilitatea.

Securitatea şi confidenţialitatea votului electronic

A. Securitatea în exploatarea votului

Pentru exploatarea în condiţii de siguranţă a modulului specific votului electronic, s-au utilizat o serie de tehnici şi tehnologii menite să asigure o securitate sporită fără a îngreuna nejustificat folosirea modulului de alegători. Menţionăm următoarele:

- ***protocol https***

Portalul IFEP folosește protocol securizat pentru transferul datelor, pentru a împiedica vizualizarea datelor pe canalul de comunicație server-client/client-server.

Portalul IFEP folosește un certificat valid, dintr-un lanț de certificare recunoscut la nivel internațional.

- ***două mecanisme de protecţie la nivel de autentificare.***

Pentru a-și putea exprima opțiunile de vot, alegătorul va utiliza o platformă electronică. Accesul la platforma electronică va putea fi realizat prin utilizarea concomitentă a două instrumente:

- , de forma [Id proiect]-[Cod generat], alocat în mod aleator, distinct pentru fiecare alegător (exemplu de cheie generată aleator **301-57556-001**);
- ărui avocat prin aplicația IFEP – Tabloul National al avocaților.

Pe lângă cele două instrumente de autentificare, utilizatorul va trebui să depășească testele furnizate de algoritmul reCAPTCHA: https://en.wikipedia.org/wiki/ReCAPTCHA

Observații:

✔ *beneficiarul va furniza consultantului o listă cu toti avocații cu drept de vot, listă ce va conține: nume, prenume, dosarul profesional, telefon, email;*

✔ *beneficiarul va asigura actualizarea registrului electoral integrat în platforma de vot, ce va conține o listă cu toți avocații cu drept de vot: nume, prenume, cod CCBE, telefon, email. Platforma dispune de instrumentele necesare pentru importul acestor date din bazele de date specifice.*

✔ *codul generat aleator se va transmite prin SMS votantului, pe numărul de mobil comunicat de beneficiar (sau cel existent in IFEP);*

✔ *în cazul în care alegătorul, din varii motive, nu intră în posesia codului de acces, acesta il poate obține fie prin helpdesk, în urma unui proces de validare a datelor, fie direct din contul avocatului, accesând portalul IFEP.*

B. Confidenţialitatea votului electronic

- ***Confidenţialitatea datelor stocate (salvate în baza de date)***

Pentru a asigura confidențialitatea datelor ce sunt stocate în baza de date, se asigură o criptare a codului de acces utilizând o secvență de criptare compusă din mai multe chei.

Exemplu de chei:

- . 1 - cunoscută doar de consultant.
- . 2 - reprezintă o secvență de text cunoscută doar de reprezentantul beneficiarului;
- țional cheia nr. 3, 4 ... n - reprezintă secvențe de text cunoscute doar de

părțile ce prezintă un interes în cadrul procedurii și au fost desemnate prin documente specifice (regulament proiect, lege, etc);

Pentru efectuarea prelucrărilor necesare, cheia nr. 2 și eventuale chei ale părților implicate, sunt active în sistem, sub forma unor chei temporare criptate, pe perioada derulării votului, după care cheile devin indisponibile.

La cererea beneficiarului, acest mecanism poate fi adaptat pentru a asigura conformitatea cu cerințele proiectului.

Consultantul își asumă responsabilitatea pentru cheia deținută de acesta. În cazul în care se contestă acuratețea opțiunilor exprimate de votanți și se solicită auditarea sistemului, pe bază de proces verbal se va putea asigura decriptarea codului votantului. Pentru decriptarea informațiilor, consultantul își asumă răspunderea doar în măsura în care codurile SHA256 ale celorlalte chei necesare pentru decriptare, sunt identice cu valorile SHA256 ce sunt salvate în baza de date.

ProjectId	Level	Amprentă SHA256	TemporaryEncryptedKey
301	KeyLevel1	6cf748744292988028b7dea07dbe8e651033a1221bdf5409dcb398a0bfffa1a1	uU1LUQGuXiX22E/AnS0TsCl/Ie3ZQVOy6Izc3KVRoIfP8tSn3IF+zVPnCzSMv4G6zLtYNkZEhOW648eootr/qA==
301	KeyLevel2	146461330a3d69753105c2a52828f351c594d04b6a5943a8160c13802b0730a1	y/a+RWjdtsXPhE9pw8VIoD9z6hZhNMVSFsfeuEho2FS+FRKx7Axi3WIt9Zj/dhNb7pDGbGb0/cVRtP2AoQjuMw==

PersonId	Status	EncryptedCodeValue
7670	Finalizat	4LTK89DKrPGaSbCtjZttDsVtI/TZc3M1sVwTzpoKrQJ6DJnwKsxkFwNdDd9+W1kW4ZwD1Q1KK9/Xy3XxZ0khpA==
7671	În lucru	

Această cheie compusă asigură criptarea codului alegătorului.

Autenticitatea optiunilor exprimate de alegător se va realiza prin utilizarea mecanismului SHA256. Astfel, pentru a avea garanția că opțiunile exprimate de alegător sunt salvate corespunzător în baza de date, alegătorul va putea verifica acest lucru, online, prin validarea amprentei SHA256 asociată opțiunilor exprimate de acesta.

După selectarea pozițiilor dorite și transmiterea votului, votantul va putea vizualiza în platformă (va primi și Email) un cod generat aleator, de tip strongpassword, compus din minim 20 de caractere.

Spre exemplu, dacă un votant are următoarele coordonate:

- Codul de acces la platforma de votare este: 301-57556-001
- Codul CCBE al votantului este: 4000-403-007-670
- Pozițiile votate de acesta sunt: 1,7,10,43,55,78,94
- Codul generat aleator, de tip strongpassword, primit la finalizarea votului: **n&&Q+Z2GvK$cQj!aPnYkC3V)XF!7anzK8@qTWhyIldgFxc9de!$eQw62pva^Iq3C**

În această situație, codul SHA256 generat de sistem va fi: c89c9733f120d9189f1a5380a3b3a9bdf2c198e9e35c7ec66ceb5d9af4959e91

Codul SHA256 va constitui amprenta textului: 301-57556-001|4000-403-007-670|n&&Q+Z2GvK$cQj!aPnYkC3V)XF!7anzK8@qTWhyIldgFxc9de!$eQw62pva^Iq3C|1,7,10,43,55,78,94

Astfel, se poate opta ca într-o secțiune disponibilă public, se fie vizibile amprentele SHA asociate codurilor de acces furnizate votanților.

Cod de acces	Status	Amprentă SHA256
301-57556-001	Finalizat	c89c9733f120d9189f1a5380a3b3a9bdf2c198e9e35c7ec66ceb5d9af4959e91
301-25451-194	În lucru	

Pentru efectuarea propriilor verificări privind integritatea amprentei electronice a opțiunilor exprimate, alegători pot folosi surse externe online precum Hash Online Calculator - https://md5file.com/calculator, sau pot folosi aplicații software dedicate (ex: HashCheckSetup - http://code.kliu.org/hashcheck/, http://www.softpedia.com/get/System/OS-Enhancements/HashCheck-Shell-Extension.shtml).

Informații suplimentare privind Sha256 pot fi găsite la adresa: https://en.wikipedia.org/wiki/SHA-2

Pentru a putea efectua prelucrările necesare centralizării voturilor, în baza de date se vor păstra următoarele informații

Cod de acces (SecurityCodeEncrypted)	Status	Poziții exprimate
LsHI5zaYKeKbXba3oFeHTH1Eg9zrRluXYkUeaX6owm0=	Finalizat	Conținut JSON cu ID-urile buletinelor de vot pe baza cărora se pot identifica pozițiile exprimate de votant, ex: 1,7,10,43,55,78,94

Important: NU se poate face o asociere între votant și codul acestuia, fără una din chei. Dacă la o dată ulterioară se dorește auditarea mecanismului de votare, lipsa oricărei chei, din cele folosite pentru criptare, face imposibilă decriptarea votului

Toate datele criptate aferente proiectului vor fi stocate pentru o perioada de 3 ani de la finalizarea votului, prin grija consultantului.

La cerere, consultantul va furniza pe suport electronic, în vederea arhivării și eventual a consultării ulterioare, jurnalele aferente proiectului. Datele furnizate vor fi criptate iar consultarea/analiza acestora de către beneficiar va putea fi efectuată doar în prezența consultantului.

Ușurința în exploatare

Interfețele utilizate în cadrul votului electronic vor fi adaptate împreună cu reprezentanți ai beneficiarului, dacă este cazul, pentru a se apropia cât mai mult de cerințele specifice ale beneficiarului și ale proiectului

Trasabilitatea acțiunilor și adaptabilitatea

În proiectarea votului electronic s-a avut în vedere ca acțiunile necesare prelucrării

voturilor să poată fi auditate.

Orice ajustare și îmbunătățire a sistemului de vot electronic se poate realiza într-un timp relativ scurt.

C. Consultarea electronica

La cerere, consultantul va asigura integrarea în platforma de vot a unor instrumente menite să permită celor interesați consultarea formei electronice a buletinelor de vot. Pentru fiecare categorie de buletine de vot, cei interesați vor putea solicita, prin intermediul IFEP, posibilitatea de a consulta forma electronică a voturilor exprimate și rezultatul interpretării prin procesare electronică. La finalizarea procedurii de vot, consultantul va putea întreprinde demersurile necesare pentru a asigura livrarea pe suport electronic a jurnalelor aferente proiectului precum și a serverelor folosite sub forma unor containere, precum: container pentru serverele de baze de date, container pentru serverele web (autentificare, cabină, notificare, registru, api), containere pentru serverele cache. Toate informațiile furnizate vor fi criptate iar consultarea/analiza acestora de către beneficiar va putea fi efectuată doar în prezența consultantului și având la bază motive întemeiate.