Colegiul Medicilor din România

Str. Pictor Alexandru Romano nr. 14, sector 2, Cod Poştal 023965, Bucureşti, RO
Cod Fiscal: 9708419; Tel: 021.413.88.00; 021.413.88.03; Fax: 021.413.77.50.
E-mail: office@cmr.ro; web: www.cmr.ro

Decizia nr. 9 din 28.04.2023

pentru aprobarea Notei tehnice privind utilizarea votului electronic

În temeiul art. 453 şi 454 din Legea nr. 95/2006 privind reforma în domeniul sănătăţii, republicată, cu modificările şi completările ulterioare, precum şi al art. 112 din Statutul Colegiului Medicilor din România, adoptat prin Hotărârea Adunării generale naţionale a Colegiului Medicilor din România nr. 1/2022 privind adoptarea Statutului şi a Codului de deontologie medicală ale Colegiului Medicilor din România, cu modificările şi completările ulterioare,

Luand in considerare dispozitiile Deciziei Consiliului national al Colegiului Medicilor din Romania nr. 8/2024 privind stabilirea datei organizării alegerilor pentru comisiile de disciplină şi pentru Comisia Superioară de Disciplină, adoptarea Regulamentului electoral şi aprobarea componenţei Comisiei Electorale Centrale,

CONSILIUL NAŢIONAL
al
COLEGIULUI MEDICILOR DIN ROMÂNIA

DECIDE:

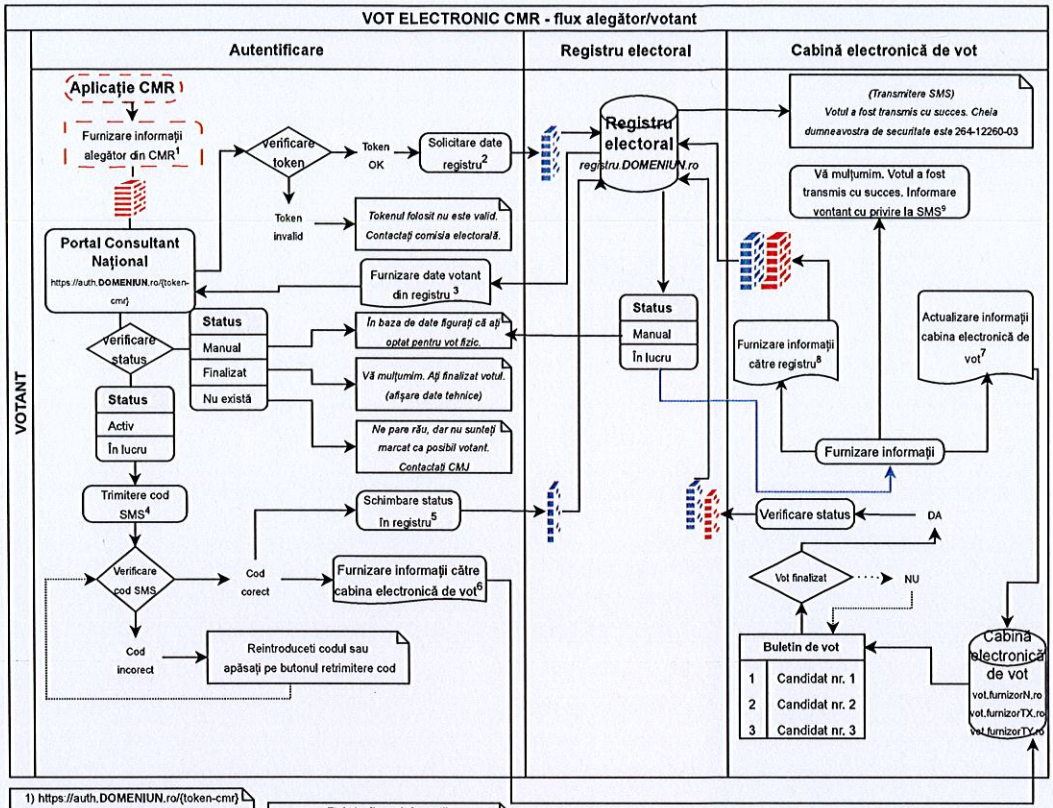
Art. 1. - Se aproba Nota tehnica privind utilizarea votului electronic prevazuta in anexa ce face parte integranta din decizie.

Art. 2. - Prezenta decizie se comunica tuturor colegiilor teritoriale.

Preşedintele Colegiului Medicilor din România,
Prof. Univ. Dr. Daniel Coriu

Colegiul Medicilor România

Bucureşti, 28 aprilie 2023.
Nr. 9



1) https://auth.DOMENIUN.ro/{token-cmr}
Token-ul CMR, codat în base64, se obține din Codul unic al medicului și o dată de valabilitate, informații criptate cu o cheie simetrică cunoscută de Consultantul IT Național și CMR

2) https://registru.DOMENIUN.ro/{token-cn}
Token-ul Consultantului IT Național, codat în base64, conține codul unic al medicului și o dată de validare, criptat cu un algoritm cunoscut doar de Consultantul IT Național.

3) Date vontant ce sunt transmise către auth.DOMENIUN.ro
a) Token votant codat în base64 ce conține codul unic al votantului, informație criptată cu ajutorul a 3 chei (cheia CMR, cheia CMJ și cheia Consultantului IT Național)
b) Nr. de mobil al votantului
c) Adresa de email a votantului
d) Adresa url a cabinei de vot
- https://vot.furnizorN.ro
- https://{vot.furnizorTX.ro}
- https://{vot.furnizorTY.ro}

4) Cod validare votant
Codul de validare al votantului va fi transmis prin sms și va fi folosit de votant pentru a trece de autentificare și a intra în cabina de vot.
(ex cod: 90334)

5) Schimbare status registru https://registru.DOMENIUN.ro/{token-votant}/status/{status nou}
(status-ul se va schimba din Activ în În lucru)

6) Accesare cabina de vot
https://{cabina de vot}/{token-cabina}
Token-cabina, codat în base64, va conține token-ul votantului și o dată de valabilitate, informații criptate cu o cheie simetrică cunoscută de Consultantul IT Național și cabină
Se va actualiza profilul votantului din cabina de vot (adăugare sau modificare) cu status În lucru

7) Actualizare informații cabina de vot, la finalizarea votului
Se va actualiza status-ul votantului din În lucru în Finalizat plus informațiile aferente votului: cheia de securitate, poziții votate, date tehnice

8) Furnizare informații către registru
API POST
- cheia de securitate a votantului
- pozitiile votate
https://api.DOMENIUN.ro/vote/complete
(status-ul se va schimba din În lucru în Finalizat)

9) Informare votant cu privire la faptul că va trebui să rețină această cheie dacă dorește să utilizeze procedura de contestare/consultare ulterioară a votului

Firewall
Metodele API folosite pentru citirea sau actualizarea registrului pot fi accesate doar din infrastructura DOMENIUN.ro

Firewall
Metodele API folosite pentru citirea sau actualizarea registrului pot fi accesate doar de pe terminale al căror IP este introdus în registru și dețin o cheie de autorizare

Cabină electronică de vot
https://vot.furnizorN.ro
https://vot.furnizorTX.ro
https://vot.furnizorTY.ro

Registru electoral 3
https://registru.DOMENIUN.ro

Tabel: Info vot

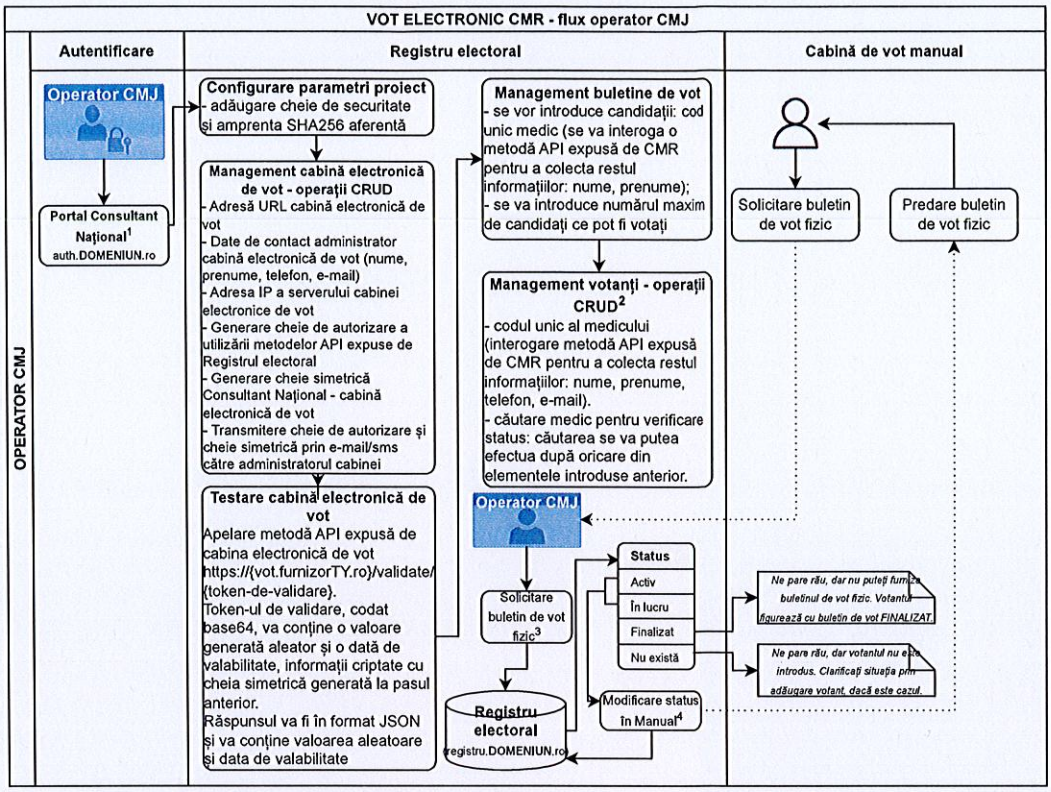
Cheie securitate votant criptată	Poziții votate criptate cu cheia cabină	Date tehnice	Status
ZkF6dnVRcjQmQFJ XclBBYWZBenZ1UXI 0JkBSV3JQQWEBt6 Mjtz4sxEkMDsG0e2bt	Lvd+wFxyxUVz2W yOui+XfRQBHt90 dnWSP2Zh6dQx+ u92NJDesqa9GG2	Ip, terminal, browser, etc	Finalizat

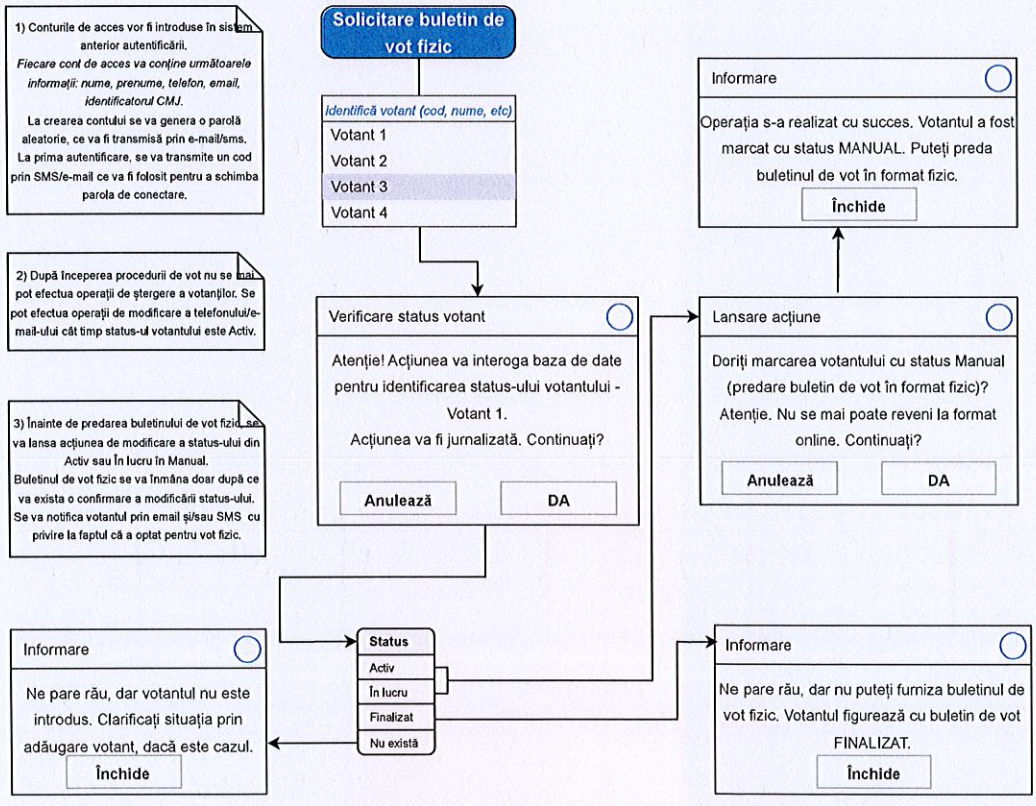
Tabel: Info votanți

Cheie securitate	Date votant	Salt aleator	Status
264-12260-03	Codul unic al medicului: *(ex: 4000-210-000-001)* Nume: Popescu Prenume: Mihai Email: xxxx@yyyy.ro Tel: +40-7XX-XXXXXX	*fAzvuQr4&@R WrPAa*	Activ

Tabel: Info vot

Identificator CMJ	Cheie securitate votant criptată cu cheia combinată	Poziții votate criptate cu cheia combinată	Date tehnice
1001	ZkF6dnVRcjQmQF XclBBYWZBenZ1U 0JkBSV3JQQWEBt Mjtz4sxEkMDsG0e2	*FAMnVow46hP mj4Wkx51ygF Gpl707M5z7 HtuK5AQ+phA GcRTI8pNWOi3 5DHN7oWNd*	Ip, terminal, browser, etc





Cerințe criptare/decriptare:

Algoritm: AES, CipherMode.CBC; Mărime cheie: 256-bit; Mărime block: 128-bit; Clasa Rfc2898DeriveBytes pentru a deriva cheia și vectorul de inițializare, folosind un salt generat aleatoriu și 10.000 de iterații.; Clasa RNGCryptoServiceProvider pentru a genera numere aleatoare pentru salt și vectorul de inițializare; Output-ul criptat codat în Base64.

Exemple flux tehnic

1. Accesare serviciu de autentificare https://auth.domeniuN.ro din aplicația CMR pentru a intra în cabina de vot

- Exemplu CUIM: 1122334455
- Exemplu cheie simetrică CMR-ConsultantNational: X!@passCmrCN123 (cunoscută de CMR și Consultantul Național)

Informațiile care trebuie transmise către sistemul de autentificare:

- CUIM|data, exemplu: 1122334455|2023-04-21 00:30:01

Informația de mai sus se criptează și se obține token-cmr.

var token-cmr = Encrypt("1122334455|2023-04-21 00:30:01","X!@passCmrCn123")

- token-ul cmr rezultat va fi codat în Base64 și va fi de forma:

LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxXRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC/7TWW9kHSc+cHbCxvQ==

-token-ul se va encoda pentru a putea fi transmis prin URL

var token = HttpUtility.UrlEncode("LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxXRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC/7TWW9kHSc+cHbCxvQ==");

- token-ul encodat rezultat va fi de forma: LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxXRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC%2F7TWW9kHSc%2BcHbCxvQ%3D%3D

- se va accesa serviciul de autentificare transmițând token-ul encodat

https://auth.domeniun.ro/token/LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxXRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC%2F7TWW9kHSc%2BcHbCxvQ%3D%3D

- la nivelul serviciului de autentificare se decriptează token-ul pentru a extrage codul CUIM:

var decodedToken = HttpUtility.UrlDecode ("LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxXRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC%2F7TWW9kHSc%2BcHbCxvQ%3D%3D")

informatia rezultata va fi: LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxXRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC/7TWW9kHSc+cHbCxvQ==

var dateCmr = Decrypt("LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxXRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC/7TWW9kHSc+cHbCxvQ==","X!@passCmrCN123")

informația rezultată va fi:1122334455|2023-04-21 00:30:01. Din această informație se va extrage CUIM și se va folosi mai departe.

2. Cheie combinată Comisia electorală centrală/CMR, Comisia electorală teritorială/CMJ și Consultant IT Național

- ex: cheie CMR: L7@22 (cunoscută doar de Comisia Electorală Centrală)*
- ex: cheie CMJ: Ax1134!24@ (cunoscută doar de Comisia electorală teritorială)*
- ex: cheie Consultant IT Național: rXax14@82 (cunoscută doar de Consultantul IT Național)*
Cheia compusă va fi L7@22Ax1134*!24@rXax14*@82*

- ex: cheie de securitate votant:264-12260-03

La adăugarea unui votant în registrul electoral, i se atașează o cheie unică de forma 264-12260-03 și i se mai atașează un text aleatoriu de 16 caractere ce va fi folosit pentru criptarea cheii de securitate. Textul aleatoriu va determina saltul pentru criptare și este necesar pentru a garanta că la fiecare utilizare a claselor de criptare, se va genera aceeași cheie criptată, dat fiind faptul că această cheie va fi ulterior folosită în cabină.
- var randomSalt = GenerateRandomPassword(16). Exemplu de salt: fAzvuQr4&@RWrPAa

Cheia de securitate criptată a votantului se va obține astfel:
- var codSecuritateVotantCriptat = Encrypt("264-12260-03","L7@22Ax1134*!24@rXax14*@82","fAzvuQr4&@RWrPAa")*
*cheia de securitate criptată a votantului va fi de forma: **ZkF6dnVRcjQmQFJXclBBYWZBenZ1UXl0JkBSV3JQQWEBt6Mjtz4sxEkMDsG0e2bt***

3. Accesare cabină

- ex: cheie simetrică Consultant IT Național-Cabină: A24&x@174! (cheie generată automat la inițierea parametrilor specifici proiectului și transmisă către administratorul cabinei, pentru configurarea cabinei). Cheia va fi folosită pentru transferul de date între Registrul electoral și Cabină.
Mod de transmitere a cheii de securitate criptată a votantului către cabină

var token-cabina = Encrypt("ZkF6dnVRcjQmQFJXclBBYWZBenZ1UXl0JkBSV3JQQWEBt6Mjtz4sxEkMDsG0e2bt|2023-04-21 00:30:30","A24&x@174!")

tokenul-cabina va arăta de forma:

DRJH9epYXkDXEKG8XkUg2s8Pa5xGOGCmekk33siQq7+SHYwpY9kynEdzo2ckAK7JRBhJ1u1euUk19KlUdjVS2VcdW7G71Gqxx2c1tCYlJMN4LQkFY2KPzHydf1b5cD2lrbQitNfamFvR1cle7Cg6mgkeTheMtay0Vr1pRiLeU=

Acest token se va encoda pentru a putea fi transmis prin URL.

4. Transmitere poziții exprimate către registrul electoral în vederea stocării

De la cabină, la finalizarea votului de către un elector, se vor transmite către registrul electoral, prin API - POST, următoarele informații:
a) cheia de securitate criptată a votantului: ex: ZkF6dnVRcjQmQFJXclBBYWZBenZ1UXl0JkBSV3JQQWEBt6Mjtz4sxEkMDsG0e2bt
b) pozițiile exprimate de acesta: ex: 1,2,8,9
Aceste informații vor fi transmise criptat către Registrul electoral (criptarea se va face cu cheia simetrică ConsultantNational-Cabină: A24&x@174!).
Odată ajunsă informația criptată la registrul electoral, aceasta se va decripta folosind cheia simetrică Consultant IT Național-Cabina, iar pozițiile exprimate se vor recripta cu cheia combinată
var pozițiiVotateCriptareRegistru = Encrypt("1,2,8,9","L7@22Ax1134*!24@rXax14*@82")*
pozitiile votate criptate cu cheia combinată vor fi de forma: FAMnVow46hPmj4Wkx51ygFGpI707M5z7HtuK5AQ+phAGcRTI8pNW0i35DHN7oWNd, iar această valoare se va salva în baza de date aferentă registrului electoral și va sta la baza centralizării rezultatelor la finalul procedurii, centralizare ce va fi verificată în oglindă cu centralizarea de la nivelul cabinei.

La nivelul cabinei, pozițiile 1,2,8,9 vor fi criptate cu cheia simetrică ConsultantNational-Cabină: A24&x@174!
var poziteiVotateCriptareCabină = Encrypt("1,2,8,9","A24&x@174!")
pozițiile votate criptate cu cheia ConsultantNational-Cabină vor fi de forma: qil0ePRAhMaA8aPvpyYorahj2vrU/UbJ31xRUWEA8w5X2N+YkqW4BT+6RVGcENHI, iar această valoare se va salva în baza de date aferentă cabinei și va sta la baza centralizării rezultatelor la finalul procedurii, centralizare ce va fi verificată în oglindă cu centralizarea de la nivelul registrului electoral.

Colegiul Medicilor România