Colegiul Medicilor din România

Str. Pictor Alexandru Romano nr. 14, sector 2, Cod Poștal 023965, București, 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 .15 din 28.07.2023

Privind completarea Deciziei Consiliului naţional al Colegiului Medicilor din România nr.9/2023 pentru aprobarea Notei tehnice privind utilizarea votului electronic

În temeiul 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, precum şi al art. 426 şi 438 din Legea nr. 95/2006 privind reforma în domeniul sănătăţii, republicată, cu modificările şi completările ulterioare,

CONSILIUL NAŢIONAL
al
COLEGIULUI MEDICILOR DIN ROMÂNIA

D E C I D E :

Art. I . Decizia Consiliului naţional al Colegiului Medicilor din România nr. 9/2023 pentru aprobarea Notei tehnice privind utilizarea votului electronic se modifică și completează după cum urmează:

1. Se aprobă propunerile tehnice ale consultanților IT desemnați de colegiile medicilor teritoriale ce și-au exprimat intenția de a utiliza propria cabină de vot electronică, propuneri ce sunt cuprinse în Anexa nr. 1 la prezenta decizie.

2. Ca urmare a propunerilor cuprinse în Anexa nr. 1 se înlocuiește Anexa la Decizia Consiliului Național al Colegiului Medicilor din România nr. 9/2023 cu Nota tehnică privind utilizarea votului electronic prevăzută în Anexa nr. 2 la prezenta decizie.

3. Consultanții IT naționali și consultanții IT teritoriali care administrează cabina electronică de vot prevăzuți la art. 57 alin 1) și 2) din Regulamentul electoral aprobat prin Decizia Consiliului naţional al Colegiului Medicilor din România nr. 8/2023, vor asigura exportul legăturii dintre ID-ul votantului, generat la nivelul registrului și ID-ul generat la nivelul cabinei, după finalizarea procedurii de vot. Fișierul exportat va fi în format excel sau JSON și se va păstra parolat pe un dispozitiv extern (memory stick). Parola de acces pentru consultarea fișierului va fi păstrată într-un plic sigilat la nivelul comisiei electorale teritoriale și va fi predată conducerii colegiului teritorial potrivit art. 103 din Regulamentul electoral, la sfârșitul procesului electoral, împreună cu stick-ul cu datele.

Art. II. Prezenta decizie se comunică tuturor colegiilor teritoriale.

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

București, 28.07.2023
Nr. 15

Daniel Coriu
Digitally signed by Daniel Coriu
Date: 2023.07.31 13:49:47 +03'00'

ANEXA NR. 1

Propunere tehnică

Urmare a discuțiilor tehnice purtate cu specialiștii IT desemnați de colegiile medicilor ce și-au exprimat intenția de a utiliza propria cabină de vot, au rezultat următoarele cerințe specifice:

1. **Anonimizarea ID-ului votantului:**

ID-ul votantului, ce va fi transmis de la registru la cabină, va fi anonimizat (eliminarea oricăror informații personale sau identificabile din identitatea votantului). La nivelul cabinei se va asigura o a doua anonimizare, cu mecanisme de secretizare ale cabinei de vot, astfel încât la nivelul registrului să nu se poată efectua desecretizarea fără o informație furnizată de la nivelul cabinei de vot.

2. **Desecretizarea votului:**

În cazul în care se decide desecretizarea voturilor, va fi necesar să se solicite cabinei furnizarea legăturii dintre ID-ul anonimizat transmis de la registru la cabină și ID-ul anonimizat generat la nivelul cabinei. Acest proces va permite asocierea votului cu ID-ul votantului și ulterior, după decriptare, folosind cheile de criptare de la nivelul registrului, se va putea aplica procedura de desecretizare stabilită prin regulament.

3. **Trimiterea voturilor:**

Transmiterea rezultatelor votului se va face la intervale definite de timp. Pentru a asigura securitatea și integritatea acestui proces, se vor aplica următoarele măsuri:

a. Se vor transmite doar rezultatele votului în cazul în care se atinge un număr minim de voturi.
b. Nu se vor transmite timestamp-uri (marcaje de timp) împreună cu rezultatele votului.
c. Rezultatele votului se vor transmite într-o ordine aleatorie, în locul transmiterii în ordine cronologică.
d. La momentul finalizării votului se va asigura transmiterea către registru a faptului că s-a finalizat votul, pentru a asigura marcarea în baza de date cu status-ul corespunzător (apelarea metodelor API specifice), în vederea evitării dublei votări (online și manual).

4. **Semnături electronice:**

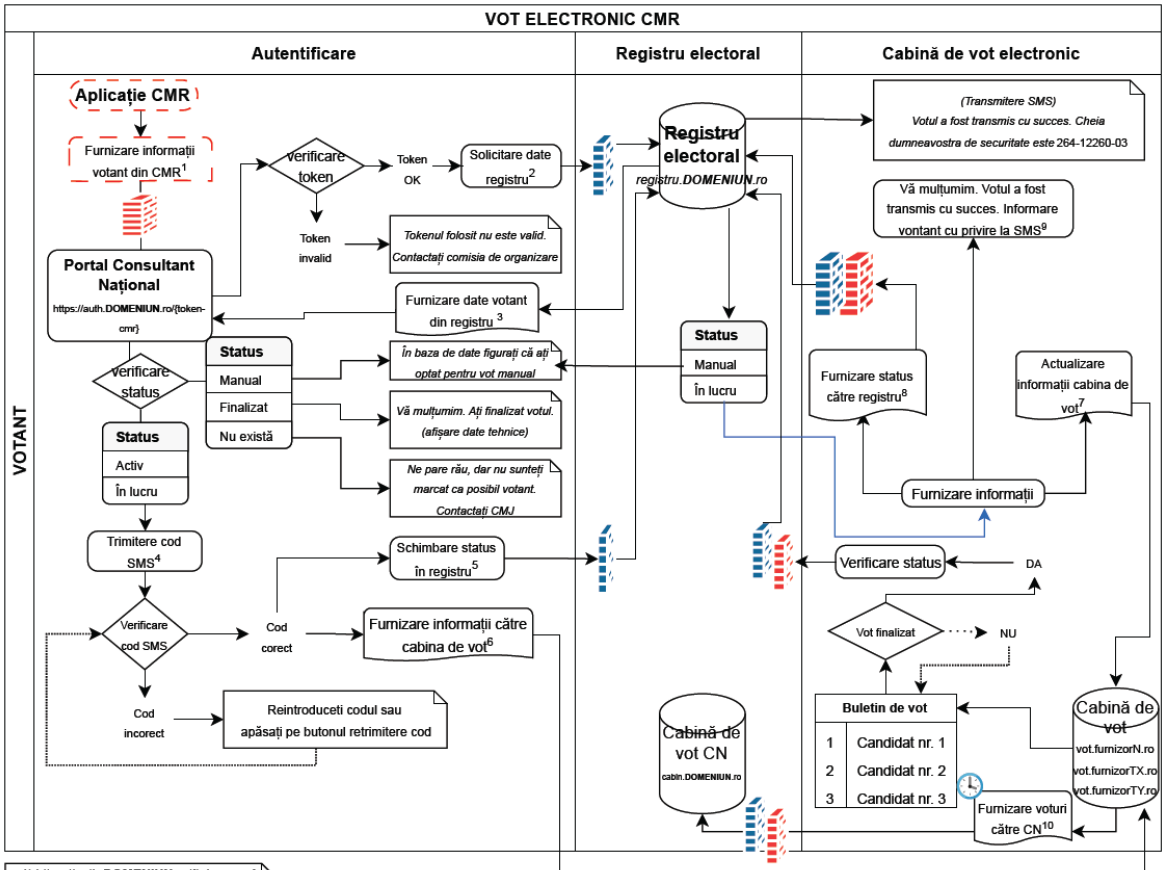
Toate voturile vor fi semnate electronic, iar pentru fiecare vot se va aștepta o semnătură electronică de la nivelul registrului.

5. **Trimiterea finală a voturilor**

La închiderea votării, toate voturile netransmise vor fi transmise în ordine aleatorie și fără timestamp-uri.

Baza de date a cabinei de vot și toate jurnalele aferente vor fi păstrate timp de **36 luni** după terminarea alegerilor, pentru eventuale verificări. Datele de la nivelul cabinei vor fi furnizate doar în cazul aplicării procedurii de desecretizare.

ANEXA NR. 2



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 status vot către registru

API POST
- cheia de securitate a votantului **de la nivelul registrului**
- status-ul votului

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

10) Furnizare informații către cabina națională, la un anumit interval de timp

API POST
- cheia de securitate a votantului **de la nivelul cabinei**
- pozitiile votate

https://api.**DOMENIUN**.ro/vote/results

Cabină de vot externă
https://vot.furnizorTX.ro
https://vot.furnizorTY.ro

Cabină de vot CN
https://cabin.**DOMENIUN**.ro

Tabel: Info vot

Cheie securitate votant (de la nivelul registrului) criptată	Cheie votant de la nivelul cabinei[11]	Poziții votate criptate cu cheia cabină	Date tehnice	Status
ZkF6dnVRcjQmQFJ XclBBYWZBenZ1UXI 0JkBSV3JQQWEBl6 Mlfz4sxEkMDsG0e2b	CM-X-223	Lvd+wFxyxUVz2W yOul+XfRQBH90 dnWSP2Zh6dQv+ u92NJDesqa9GG2	Ip, terminal, browser, etc	Finalizat

Tabel: Info vot

Cheie securitate votant (de la nivelul registrului) criptată	Cheie votant de la nivelul cabinei[11]	Poziții votate criptate cu cheia combinată	Date tehnice	Status
ZkF6dnVRcjQmQFJ XclBBYWZBenZ1UXI 0JkBSV3JQQWEBl6 Mlfz4sxEkMDsG0e2b	CM-X-223	Lvd+wFxyxUVz2W yOul+XfRQBH90 dnWSP2Zh6dQv+ u92NJDesqa9GG2	Ip, terminal, browser, etc	Finalizat

11) În cazul cabinei externe, se va asigura furnizarea legăturii între cheia de securitate a votantului de la nivelul registrului și cheia votantului de la nivelul cabinei, **doar** în caz de contestație, conform regulamentului

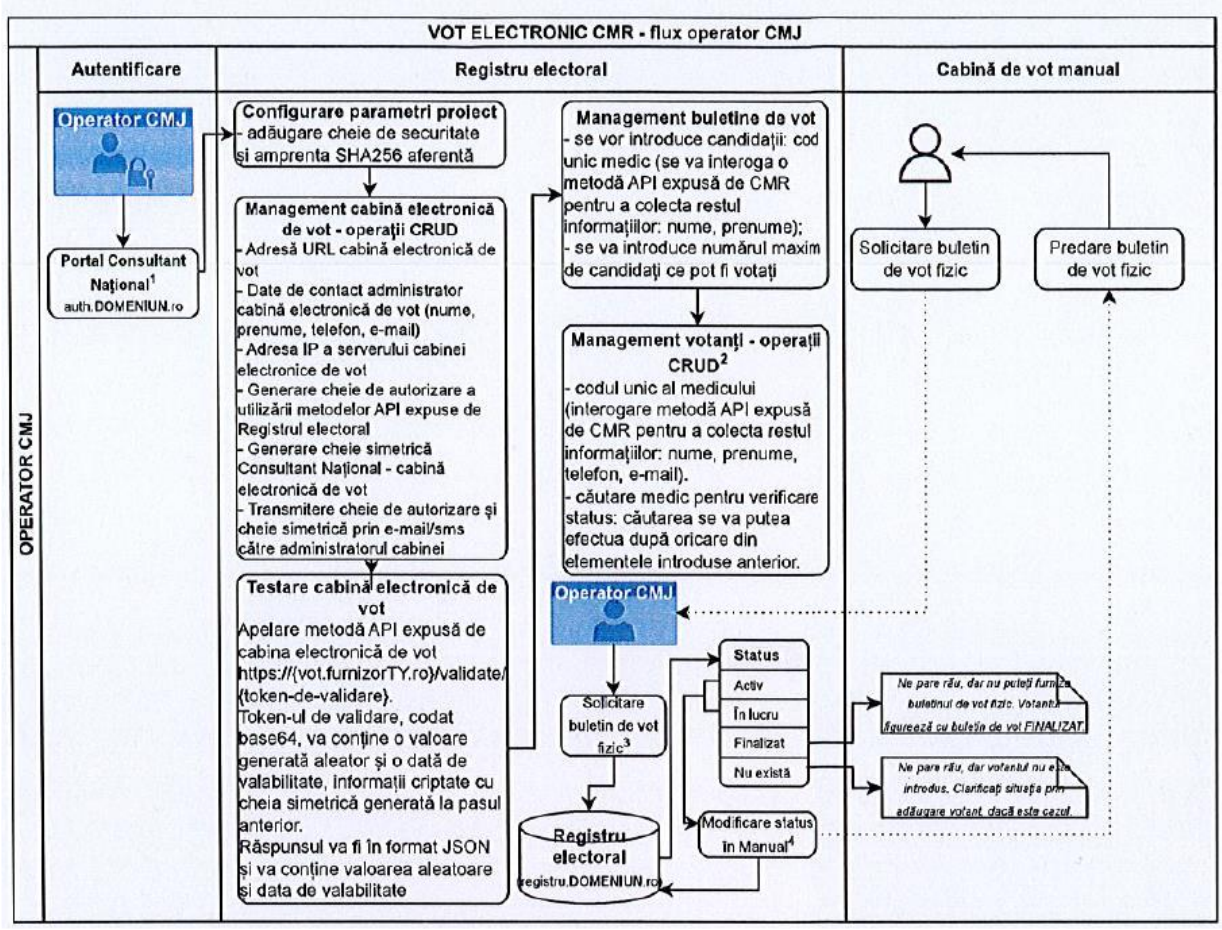
Firewall
*Metodele API folosite pentru citirea sau actualizarea registrului pot fi accesate doar din infrastructura **DOMENIUN**.ro*

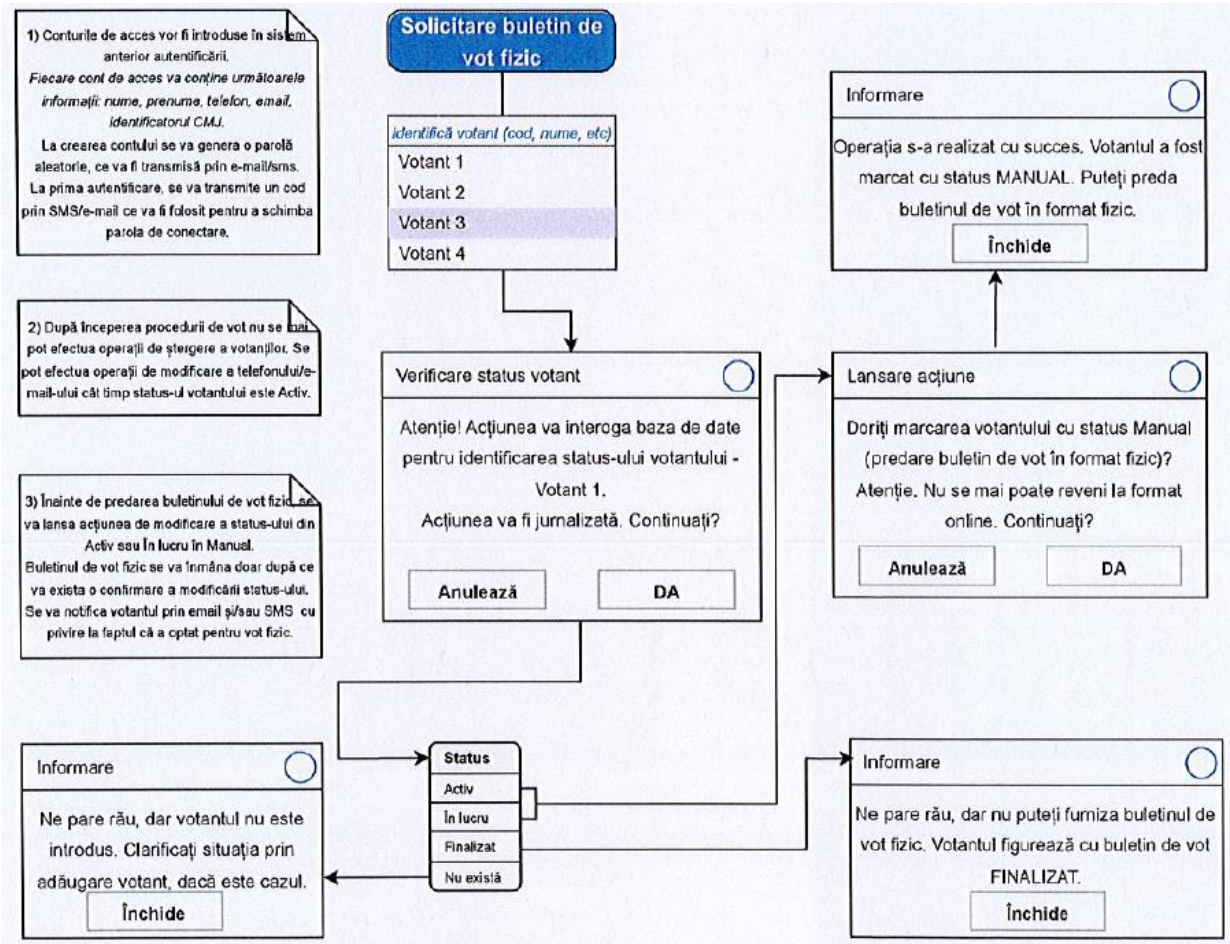
Firewall
Metodele API folosite pentru citirea sau actualizarea registrului pot fi accesate doar de pe terminale al căror IP este introdus în registru și dețin o cheie de autorizare

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

Tabel: Info votanți

Cheie securitate	Date votant	Salt aleator	Status
264-12260-03	Codul unic al medicului: *(ex: 8098708970897)* Nume: Popescu Prenume: Mihai Email: xxxx@yyyy.ro Tel: +40-7XX-XXXXXX	*fAzvuQr4&@R WrPAa*	Activ


VOT ELECTRONIC CMR - flux operator CMJ
OPERATOR CMJ
Autentificare
Registru electoral
Cabină de vot manual
Operator CMJ
Portal Consultant Național[1]
auth.DOMENIUN.ro
Configurare parametri proiect
- adăugare cheie de securitate și amprenta SHA256 aferentă
Management cabină electronică de vot - operații CRUD
- Adresă URL cabină electronică de vot
- Date de contact administrator cabină electronică de vot (nume, prenume, telefon, e-mail)
- Adresa IP a serverului cabinei electronice de vot
- Generare cheie de autorizare a utilizării metodelor API expuse de Registrul electoral
- Generare cheie simetrică Consultant Național - cabină electronică de vot
- Transmitere cheie de autorizare și cheie simetrică prin e-mail/sms către administratorul cabinei
Testare cabină electronică de vot
Apelare metodă API expusă de cabina electronică de vot https://{vot.furnizorTY.ro}/validate/{token-de-validare}.
Token-ul de validare, codat base64, va conține o valoare generată aleator și o dată de valabilitate, informații criptate cu cheia simetrică generată la pasul anterior.
Răspunsul va fi în format JSON și va conține valoarea aleatoare și data de valabilitate
Management buletine de vot
- se vor introduce candidații: cod unic medic (se va interoga o metodă API expusă de CMR pentru a colecta restul informațiilor: nume, prenume);
- se va introduce numărul maxim de candidați ce pot fi votați
Management votanți - operații CRUD[2]
- codul unic al medicului (interogare metodă API expusă de CMR pentru a colecta restul informațiilor: nume, prenume, telefon, e-mail).
- căutare medic pentru verificare status: căutarea se va putea efectua după oricare din elementele introduse anterior.
Operator CMJ
Solicitare buletin de vot fizic[3]
Registru electoral
registru.DOMENIUN.ro
Status
Activ
În lucru
Finalizat
Nu există
Modificare status în Manual[4]
Solicitare buletin de vot fizic
Predare buletin de vot fizic
Ne pare rău, dar nu puteți fumiza buletinul de vot fizic. Votantul figurează cu buletin de vot FINALIZAT.
Ne pare rău, dar votantul nu este introdus. Clarificați situația prin adăugare votant, dacă este cazul.


1) Conturile de acces vor fi introduse în sistem anterior autentificării.
Fiecare cont de acces va conține următoarele informații: nume, prenume, telefon, email, identificatorul CMJ.
La crearea contului se va genera o parolă aleatorie, ce va fi transmisă prin e-mail/sms.
La prima autentificare, se va transmite un cod prin SMS/e-mail ce va fi folosit pentru a schimba parola de conectare.
2) După începerea procedurii de vot nu se mai pot efectua operații de ștergere a votanților. Se pot efectua operații de modificare a telefonului/e-mail-ului cât timp status-ul votantului este Activ.
3) Înainte de predarea buletinului de vot fizic se va lansa acțiunea de modificare a status-ului din Activ sau În lucru în Manual.
Buletinul de vot fizic se va înmâna doar după ce va exista o confirmare a modificării status-ului.
Se va notifica votantul prin email și/sau SMS cu privire la faptul că a optat pentru vot fizic.
Solicitare buletin de vot fizic
identifică votant (cod, nume, etc)
Votant 1
Votant 2
Votant 3
Votant 4
Verificare status votant
Atenție! Acțiunea va interoga baza de date pentru identificarea status-ului votantului - Votant 1.
Acțiunea va fi jurnalizată. Continuați?
Anulează
DA
Lansare acțiune
Doriți marcarea votantului cu status Manual (predare buletin de vot în format fizic)?
Atenție. Nu se mai poate reveni la format online. Continuați?
Anulează
DA
Informare
Operația s-a realizat cu succes. Votantul a fost marcat cu status MANUAL. Puteți preda buletinul de vot în format fizic.
Închide
Status
Activ
În lucru
Finalizat
Nu există
Informare
Ne pare rău, dar votantul nu este introdus. Clarificați situația prin adăugare votant, dacă este cazul.
Închide
Informare
Ne pare rău, dar nu puteți fumiza buletinul de vot fizic. Votantul figurează cu buletin de vot FINALIZAT.
Închide

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)

Informatiile 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 decripteaza 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 CMR, CMJ si Consultant National

- ex: cheie CMR: L7@22 (cunoscută doar de CMR)*
- ex: cheie CMJ: Ax1134!24@ (cunoscută doar de CMJ)*
- ex: cheie ConsultantNational: rXax14@82 (cunoscută doar de ConsultantulNational)*

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 asigura 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: ***ZkF6dnVRcjQmQFJXclBBYWZBenZ1UXI0JkBSV3JQQWEBt6Mjtz4sxEkMDsG0e2bt***

3. Accesare cabină

- ex: cheie simetrică ConsultantNational-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("ZkF6dnVRcjQmQFJXclBBYWZBenZ1UXI0JkBSV3JQQWEBt6Mjtz4sxEkMDsG0e2bt|2023-04-21 00:30:30","A24&x@174!")

tokenul-cabina va arăta de forma:

DRJH9epYXkDXEKG5XkUg2s5Fa5xGOGCmekk33s/Qq7+SHYwsY9kynEdzo2ckAK7JRBhJ1u1euUk19KIUdjVS2VcldW7G71Gqxx2c1tCYIJMN4LQkFY2KPzHydf1b5cD2lrbQtNfam/FvR1cle7Cg5mgkeTheMjtay0Vr1pRILeU=

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 va transmite către registrul electoral, prin API - POST, următoarele informații:

-La finalizarea votului:
a) cheia de securitate criptată a votantului: ex: ZkF6dnVRcjQmQFJXclBBYWZBenZ1UXI0JkBSV3JQQWEBt6Mjtz4sxEkMDsG0e2bt
b) status-ul votului: Finalizat. In acest fel se evită votul multiplu (online și manual)

- La intervale succesibe de timp
a) cheia votantului generată la nivelul cabinei
b) pozițiile exprimate de votant în format JSON, semnat electronic

Observație: în caz de contestație, se va furniza de la nivelul cabinei legătura dintre cheia de securitate criptată a votantului și cheia generată la nivelul cabinei.

Aceste informații vor fi transmise criptat către Registrul electoral (criptarea se va face cu cheia simetrică ConsultantNational-Cabină: ex: A24&x@174!).

Odată ajunsă informația criptată la registrul electoral, aceasta se va decripta folosind cheia simetrică ConsultantNational-Cabina, iar pozițiile exprimate se vor recripta cu cheia combinată

var pozitiiVotateCriptareRegistru = Encrypt("1,2,8,9","L7@22Ax1134*!24@rXax14*@82")*

pozitiile votate criptate cu cheia combinată vor fi de forma: FAMnVow46hPmj4Wkx51ygFGpl707M5z7HtuK5AQ+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 pozitiiVotateCriptareCabină = Encrypt("1,2,8,9","A24&x@174!")

pozițiile votate criptate cu cheia ConsultantNational-Cabină vor fi de forma: qiI0ePRAhMaA8aPvpyYorahj2vrU/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.