

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 național 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 naționale a Colegiului Medicilor din România nr. 1/2022 privind adoptarea Statutului și a Codului de deontologie medicală ale Colegiului Medicilor din România, cu modificările și completările ulterioare, precum și al art. 426 și 438 din Legea nr. 95/2006 privind reforma în domeniul sănătății, republicată, cu modificările și completările ulterioare,

CONSILIUL NAȚIONAL al COLEGIULUI MEDICILOR DIN ROMÂNIA

DE C I D E :

Art. I. Decizia Consiliului național 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 național 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.

**Președintele Colegiului Medicilor din România,
Prof. Univ. Dr. Daniel Coriu**

București, 28.07.2023

Nr. 15

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).

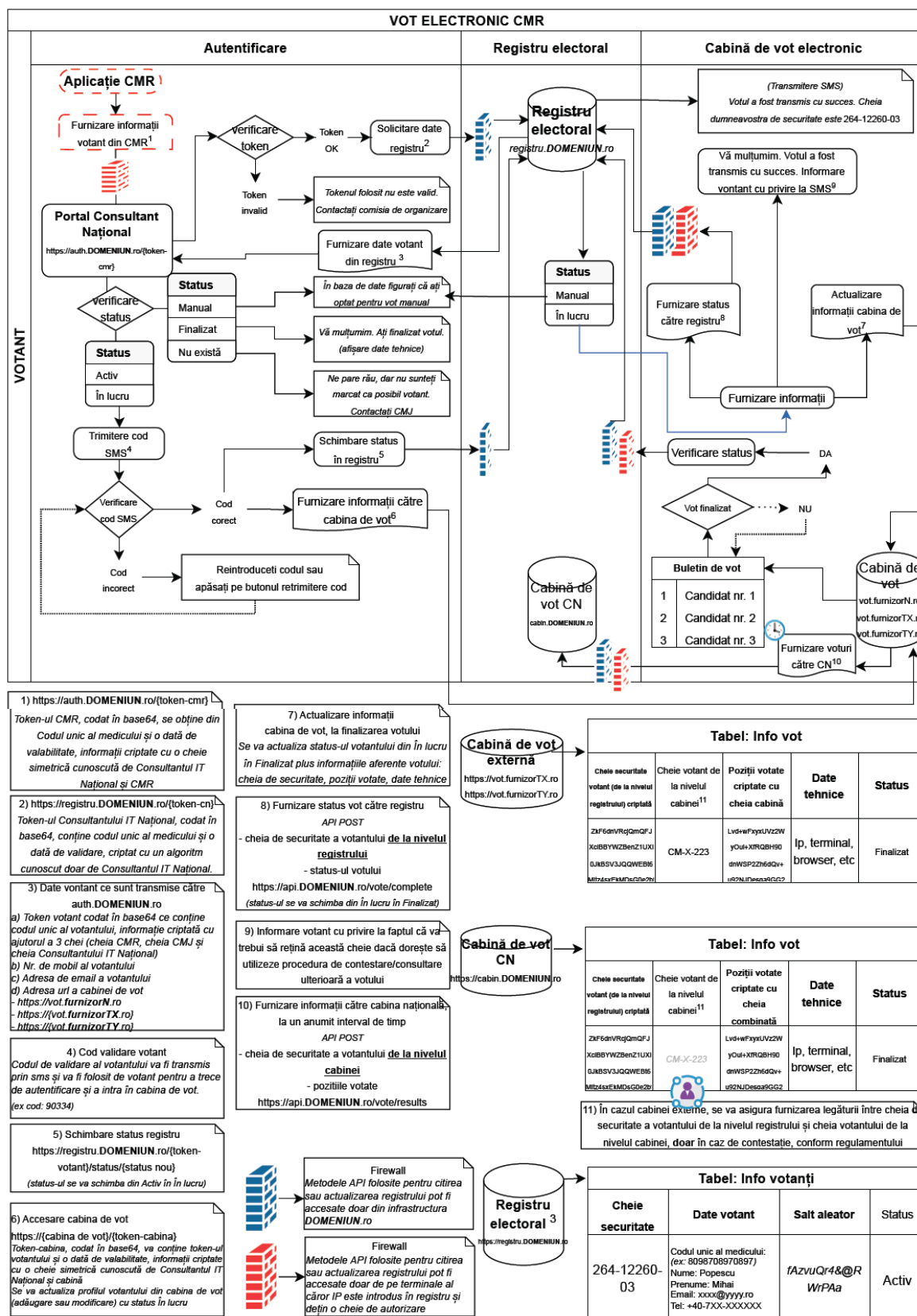
4. Semnături electronice:

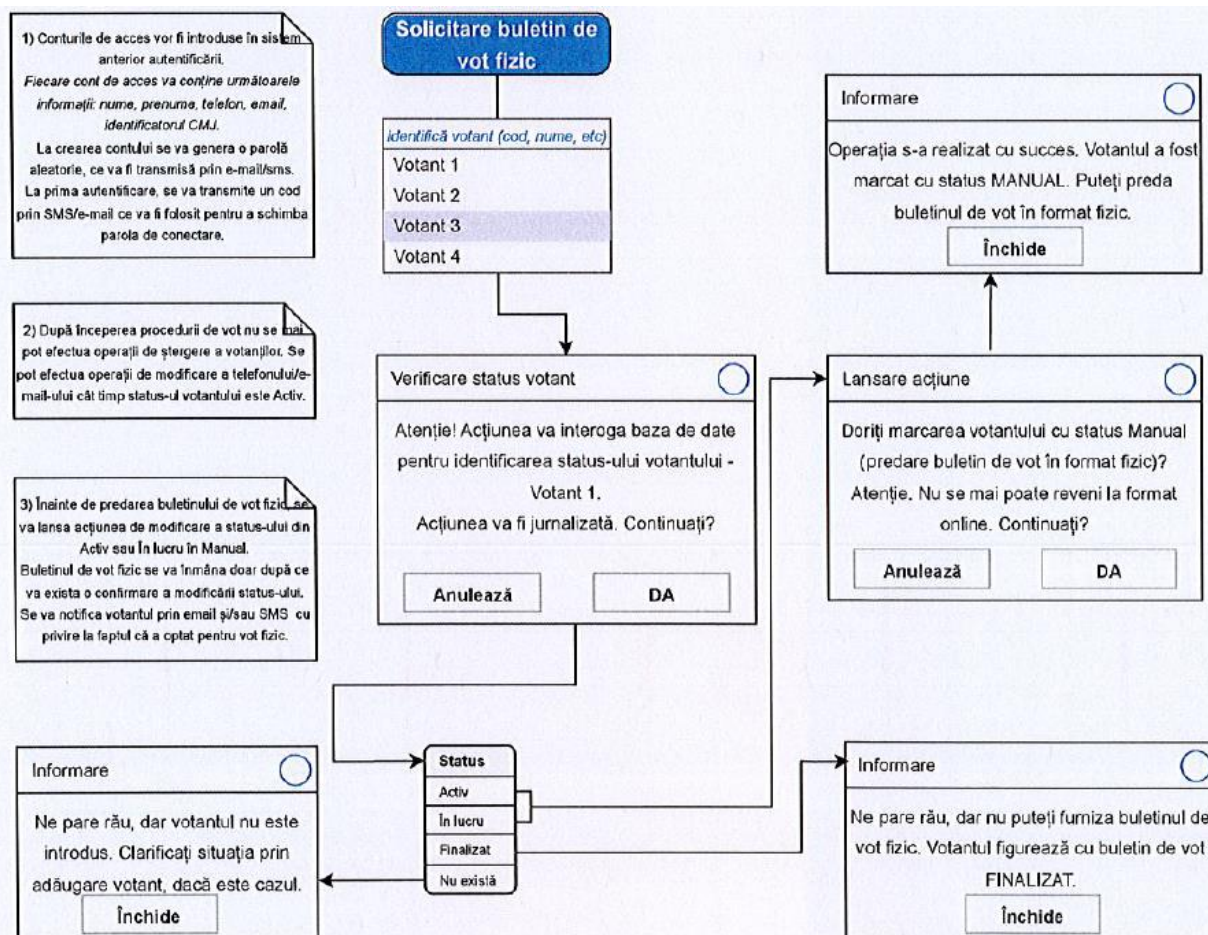
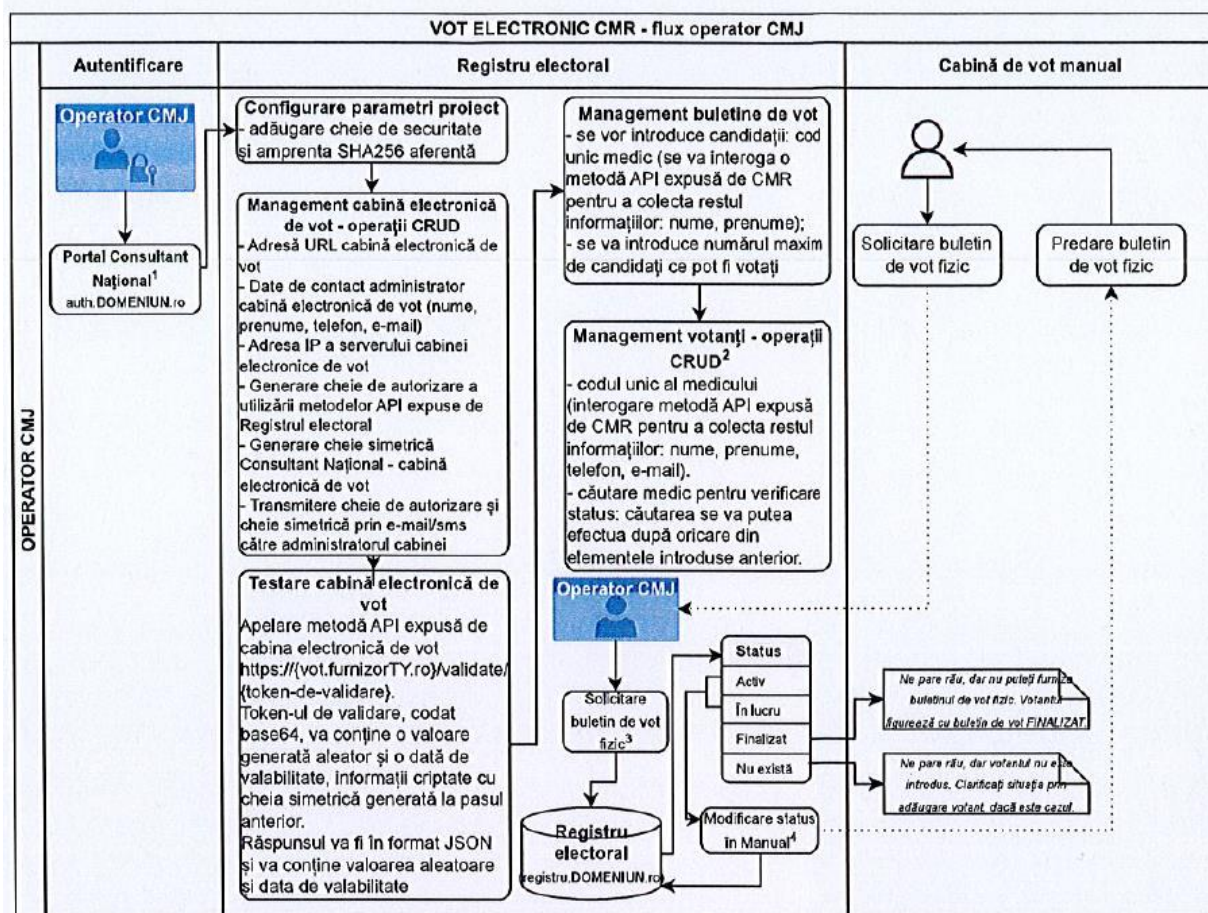
Toate voturile vor fi semnate electronic, iar pentru fiecare vot se va aștepta o semnătură electronică de la nivelul registrului.

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.





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:

`LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC/7TWW9kHSc+cHbCxxQ==`

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

`var token = HttpUtility.UrlEncode("LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC/7TWW9kHSc+cHbCxxQ==");`

- token-ul encodat rezultat va fi de forma: `LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC%2F7TWW9kHSc%2BcHbCxxQ%3D%3D`

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

`https://auth.domeniun.ro/token/LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC%2F7TWW9kHSc%2BcHbCxxQ%3D%3D`

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

`var decodedToken = HttpUtility.UrlDecode("LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC%2F7TWW9kHSc%2BcHbCxxQ%3D%3D");`

informația rezultată va fi: `LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC/7TWW9kHSc+cHbCxxQ==`

`var dataCmr = Decrypt("LLhu7YmNdRFYXO5zLYdb34zeaP7BRhSB8lxRD05sNbu9CSXrJqNcQvcqOMfF2QjANDC/7TWW9kHSc+cHbCxxQ==", "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 și 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 Consultantul National)

Cheie 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&@RWfPAa

Cheie de securitate criptată a votantului se va obține astfel

- var codSecuritateVotantCriptat = Encrypt("264-12260-03", "L7*!@22Ax1134*24@rXax14*!@82", "fAzvuQr4&@RWfPAa")

cheia de securitate criptată a votantului va fi de forma: `ZkF6dnVRqjQmQFJXclBBYWZBenZ1UX0JkBSV3JQQWEBt6Mjtz4sxEkMDsG0e2bt`

3. Accesare cabină

- ex: cheie simetrică ConsultantNational-Cabină: A24&x@174! (cheie generată automat la inițierea parametrilor specifice 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("ZkF6dnVRqjQmQFJXclBBYWZBenZ1UX0JkBSV3JQQWEBt6Mjtz4sxEkMDsG0e2bt|2023-04-21 00:30:30", "A24&x@174!")`

tokenul-cabina va arăta de forma:

`DRJh9epY0x0XK950Xug2sP5e5G0C0meK33sQqT+SHYXpY9KynEdzo2ckAK7JRBhJ1u1euUk12K0UqV52VclW7B71Gox2c11CvUJmN4LQKFY2KFzHydflbScD2VbQ8VfemFvR1cle7Cg0mpleTheIltay0V1pRLeU=`

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: `ZkF6dnVRqjQmQFJXclBBYWZBenZ1UX0JkBSV3JQQWEBt6Mjtz4sxEkMDsG0e2bt`

b) status-ul votului: Finalizat. În acest fel se evită votul multiplu (online și manual)

- La intervale succesive 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-Cabină, iar pozițiile exprimate se vor recripta cu cheia combinată

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

pozițiile votate criptate cu cheia combinată vor fi de forma: `FAMhVow46hPmj4Wkx51ygFGpl707M5z7HtuK5AQ+phAGoRT18pNW0i35DHN7oWnD`, 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: `qil0ePRAHMaA8aPvpyYorahj2vruUbuJ31xRUWEA8v5X2N+YkqW4BT+6RVGcENHl`, 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.