# CAIET DE SARCINI

**pentru elaborarea**
**Sistemului Informațional e-Votare**

**Chișinău – 2023**

**Cuprins**

# 1 Introducere

În prezent, cetățeanul folosește produsele tehnologiilor informaționale (TI) pentru o serie de activități cotidiene. Acestea îi folosesc pentru a-și gestiona finanțele personale, pentru a călători, pentru educație sau comunicare. Totodată, aceleași tehnologii oferă noi canale de comunicare între cetățeni și autoritățile publice, astfel pot fi accesate un șir de servicii publice (solicitarea de perfectarea a actelor de identitate, perfectarea unor contracte de prestări servicii, achitarea diferitor facturi, servicii, etc.) , pot fi organizate audieri on-line sau urmărirea procesului legislativ. Utilizarea tehnologiilor informaționale devine o necesitate și o posibilitate de planificare și economisire a timpului, dar și o siguranță a serviciilor pe care le utilizează.

Un alt factor important este numărul mare de alegători care votează în afara Republicii Moldova. În cadrul alegerilor parlamentare din 2019 și 2021, precum și la alegerile prezidențiale din 2020, numărul de alegători din afara țării a crescut constant generând presiune pe secțiile de votare deschise în străinătate. Au fost raportate situații când alegătorii stăteau în rând și câteva ore pentru a intra în secțiile de votare. Pandemia globală a fost o altă provocare pentru procesul electoral și a demonstrat încă o dată importanța tehnologizării mai multor procese. Astfel, procesul de vot în perioada pandemiei a fost regândit pentru a reduce contactul între oameni și pentru a fluidiza procesul în secțiile de votare.

Organizarea alegerilor a cunoscut o serie de modificări în scopul implementării tehnologiilor informaționale. În sectorul electoral din Republica Moldova au fost implementate soluții TI care și-au demonstrat eficiența. Astfel, Comisia Electorală Centrală (CEC) utilizează Sistemul informațional automatizat de stat "Alegeri" (SIASA) prin care se colectează date despre prezența la vot, precum și se colectează rezultatele preliminare ale alegerilor, ambele fiind vizualizate în regim online pe site-ul CEC-ului. De asemenea, prezența la vot se înregistrează direct în baza de date gestionată de către CEC. La intrarea în secția de votare, alegătorul prezintă operatorului de calculator actul de identitate, acesta introduce în sistem datele personale ale alegătorului și astfel se înregistrează prezența la vot. CEC menține mai multe baze de date electronice, acestea fiind Registrul de stat al alegătorilor, Registrul funcționarilor electorali, Buletinul de vot, Liste de subscripție precum și sistemul de evidență a deținătorilor de mandate (deputat, primar, consilier local) precum și a candidaților supleanți la aceste funcțiile.

În acest context, dezvoltarea și implementarea sistemului de vot prin internet reprezintă pasul următor în digitalizarea procesului de vot.

# 2 Informație generală

## 2.1 Scopul proiectului

Scopul proiectului este întocmirea prezentului Caiet de Sarcini privind crearea unui Sistem Informațional pentru Votul prin Internet (în continuare – SI e-Votare) care urmează a fi creat sub auspiciile CEC, deținut și administrat ca parte componentă a Sistemul Informațional Automatizat de Stat "Alegeri" (SIASA) de către CEC.

SI e-Votare va fi utilizat de CEC în calitate de opțiune alternativă de vot prin Internet (e-votare) la alegeri și referendumuri.

Pentru implementarea mecanismelor de votare prin internet urmează ca în Codul electoral să fie introdus un nou capitol – „Votarea prin internet". În particular, în acest capitol se va menționa că:

- Procesul de votare prin internet se va desfășura pe durata a 3 zile, de luni până miercuri, în săptămâna înainte zilei alegerilor.
- Alegătorul își poate exercita dreptul de vot prin internet de mai multe ori, doar ultimul vot fiind numărat și validat. Dacă alegătorul care a votat prin internet, merge la secția de votare și își exprimă votul utilizând buletinul de vot din hârtie, votul prin internet este anulat.

Votarea prin internet reprezintă un proces de exercitare a dreptului de vot prin intermediul unei platforme accesibile prin utilizarea internetului, cu utilizarea mijloacelor de identificare electronică a alegătorului. La fel ca votul tradițional pe hârtie, votul prin internet se realizează prin 2 pași:

1) identificarea alegătorului în baza unui act de identitate compatibil cu sistemele de identificare electronică;
2) exprimarea votului prin internet.

În cadrul arhitecturii IT a Comisiei Electorale Centrale, votul prin internet va fi asigurat de către SI e-Votare, parte componentă a sistemului informațional SIASA.

## 2.2 Referințe și aspecte legale pentru elaborarea sistemului informațional

### 2.2.1 Legislația electorală a Republicii Moldova și cadru normativ internațional

Elaborarea și aplicarea în Republica Moldova a unui sistem de vot prin internet trebuie să respecte principiile de bază ale oricărui sistem electoral prevăzut atât în legislația națională, cât și în actele internaționale.

1) Codul Electoral al Republicii Moldova;
2) Legea nr. 101 cu privire la Conceptul Sistemului informațional automatizat de stat "Alegeri" (SIASA);
3) CONCEPTUL sistemului de vot prin internet „e-Votare";
4) Recomandarea Comitetului de Miniștri al Consiliului Europei (2004 și 2017) privind standardele juridice, operaționale și tehnice pentru votul electronic.

### 2.2.2 Acte de reglementare a inițiativelor TIC a Republicii Moldova

La elaborarea SI e-Votare este oportună luarea în considerație și implementarea cerințelor și recomandărilor conținute în actele normativ-legislative privind inițiativele TIC ale Republicii Moldova. Întru respectarea cadrului de guvernare electronică promovat de Guvern trebuie să fie luate în considerație următoarele acte:

1) Hotărârea Guvernului nr. 7104 din 20.09.2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare), Monitorul Oficial Nr. 156-159 din 23.09.2011;
2) Hotărârea Guvernului nr. 128 din 20.02.2014 privind platforma tehnologică guvernamentală comună (MCloud), Monitorul Oficial Nr. 47-48 din 25.02.2014;
3) Hotărârea Guvernului nr. 656 din 05.09.2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate, Monitorul Oficial Nr. 186-189 din 07.09.2012;
4) Hotărârea Guvernului nr. 1090 din 31.12.2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), Monitorul Oficial Nr. 4-8 din 10.01.2014;
5) Hotărârea Guvernului nr. 405 din 02.06.2014 privind serviciul electronic guvernamental integrat de semnătură digitală (MSign), Monitorul Oficial Nr. 147-151 din 06.06.2014;
6) Hotărârea Guvernului nr. 708 din 28.08.2014 privind serviciul electronic guvernamental de jurnalizare (MLog), Monitorul Oficial Nr. 261-267 05.09.2014;
7) Hotărârea Guvernului Nr. 916 din 06.08.2007 cu privire la Concepția Portalului Guvernamental, Monitorul Oficial Nr. 127-130/952 din 17.08.2007;
8) Hotărârea Guvernului nr. 330 din 28.05.2012 cu privire la crearea și administrarea portalului guvernamental unic al serviciilor publice, Monitorul Oficial Nr. 104-108 din 01.06.2012;
9) Legea Nr. 91 din 29.05.2014 cu privire la semnătura electronică și documentul electronic, Monitorul Oficial Nr. 174-177 din 04.07.2014;
10) Hotărârea Guvernului Nr. 945 din 05.09.2005 cu privire la centrele de certificare a cheilor publice, Monitorul Oficial Nr. 123-125 din 16.09.2005;
11) Hotărârea Guvernului Nr. 320 din 28.03.2006 pentru aprobarea Regulamentului privind modul de aplicare a semnăturii digitale în documentele electronice ale autorităților publice, Monitorul Oficial Nr. 51-54 din 31.03.2006;
12) Hotărârea Guvernului nr. 404 din 2 iunie 2014 „Cu privire la pilotarea platformei de interoperabilitate”;
13) Hotărârea Guvernului nr.753 din 14 iunie 2016 „Pentru aprobarea Conceptul mecanismului de gestionare și eliberare a actelor permisive și a Planului de acțiuni privind implementarea soluțiilor de ghișeu unic”.

### 2.2.3 Acte generale aferente punerii în producție și funcționării SI e-Votare:

Adițional la actele juridice și normative în baza cărora trebuie să fie dezvoltat și implementat SI e-Votare, trebuie luate în considerație un set de acte juridice care impun măsuri organizaționale și constrângeri externe de funcționare a sistemului informatic. La această categorie de acte de care trebuie să țină cont SI e-Votare se poate de menționat:

1) Legea Nr. 467-XV din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat, Monitorul Oficial nr. 6-12/44 din 01/01/2004;
2) Legea Nr. 71 din 22.03.2007 cu privire la registre, Monitorul Oficial Nr. 70-73 din 25.05.2007;
3) Legea Nr. 982-XIV din 11.05. 2000 privind accesul la informație, Monitorul Oficial Nr. 88 art. Nr. 664 din 28.07.2000;
4) Legea Nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal, Monitorul Oficial Nr. 171-175 din 14.10.2011;
5) Hotărârea Guvernului Nr. 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, Monitorul Oficial Nr. 254-256 din 24.12.2010;
6) Hotărârea Guvernului Nr. 945 din 05.09.2005 cu privire la centrele de certificare a cheilor publice, Monitorul Oficial Nr. 123-125 din 16.09.2005;
7) Legea Nr. 1069-XIV din 22.06.2000 cu privire la informatică, Monitorul Oficial Nr. 073 din , 05.07.2001;
8) Legea Nr. 241-XVI din 15.11.2007 privind telecomunicațiile, Monitorul Oficial Nr. 51-54 din 14.03.2008;
9) Hotărârea Guvernului Nr. 967 din 09.08.2016 cu privire la mecanismul de consultare publică cu societatea civilă în procesul decizional, Monitorul Oficial Nr. 265-276 din 19.08.2016;
10) Hotărârea Guvernului Nr. 840 din 26.07.2004 cu privire la crearea Sistemului de telecomunicații al autorităților administrației publice, Monitorul Oficial Nr. 130 din 30.07.2004;
11) Hotărârea Guvernului Nr. 735 din 11.06.2002 cu privire la sistemele speciale de telecomunicații ale Republicii Moldova, Monitorul Oficial Nr. 79-81 din 20.06.2002;
12) Alte legi, acte normative, standarde în vigoare în domeniul TIC.

## 2.3 Acronime și noțiuni utilizate

### 2.3.1 Acronime

În prezentul document se vor utiliza următoarele acronime:

| ID | Noțiune | Descriere |
|---|---|---|
| **1** | TI | Tehnologie informatică |
| **2** | TIC | Tehnologie Informatică și de Comunicație |
| **3** | CEC | Comisia Electorală Centrală |
| **4** | RSA | Registrul de Stat al Alegătorilor |
| **5** | SIASA | Sistemul Informațional Automatizat de Stat ”Alegeri” |
| **6** | CE | Circumscripție Electorală |
| **7** | SV | Secție de Votare |
| **8** | CEE | Circumscripție Electorală Electronică |
| **9** | PDD | Portalul Datelor Deschise |
| **10** | BF | Bloc Funcțional |
| **11** | CU | Caz de Utilizare (Use Case) |
| **12** | HSM | Hardware Security Module |
| **13** | PKCS | Public Key Cryptography Standards |

### 2.3.2 Noțiuni

În prezentul document se vor utiliza următoarele noțiuni:

| ID | Noțiune | Descriere |
|---|---|---|
| **1** | Bază de Date | Ansamblu de date organizate conform structurii conceptuale care descrie caracteristicele de bază și relația dintre entități |
| **2** | Credențiale | Set de atribute ce stabilesc identitatea și autenticitatea utilizatorilor și sistemelor în cadrul sistemelor informaționale. |
| **3** | Date | Unități informaționale elementare despre persoane, subiecte, fapte, evenimente, fenomene, procese, obiecte, situații etc. prezentate într-o formă care permite notificarea, comentarea și procesarea lor. |
| **4** | Date cu caracter personal | Orice informație cu referire la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). În acest sens o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale |
| **5** | Integritatea datelor | Stare a datelor, când acestea își păstrează conținutul și sunt interpretate univoc în cazuri de acțiuni aleatorii. Integritatea se |

| | | |
|---|---|---|
| | | consideră păstrată dacă datele nu au fost alterate sau deteriorate (șterse). |
| **6** | Jurnalizare | Funcție de înregistrare a informației despre evenimente. În cadrul sistemelor informaționale înregistrările despre evenimente includ detalii despre data și ora, utilizatorul, acțiunea întreprinsă. |
| **7** | Metadate | Modalitate de atribuire de valoare semantică datelor stocate în baza de date (date despre date). |
| **8** | Obiect informațional | Reprezentare virtuală al entităților materiale și nemateriale existente. |
| **9** | Resursă informațională | Set de informație documentată în sistemul informatic, menținut în concordanță cu cerințele și legislația în vigoare |
| **10** | Sistem informatic automatizat (SIA) | Ansamblu de programe și echipamente care asigură prelucrarea automată a datelor (componenta automatizată a sistemului informațional). |
| **11** | Sistem Informațional (SI) | Sistem de prelucrare a informației, împreună cu resursele organizaționale asociate, cum ar fi resursele umane și tehnice, care furnizează și distribuie informația. |
| **12** | Tehnologie informatică și de comunicație (TIC) | Termen comun care include toate tehnologiile utilizate pentru schimbul și manipularea informației. |
| **13** | Software Design Document (SDD) | Document director al sistemului informatic care cuprinde descrierea detaliată a următoarelor viziuni: structurile de date și constrângerile acestora, arhitectura sistemului informatic care oferă totalitatea secțiunilor conceptuale ale sistemului informatic, interfața sistemului informatic care cuprinde conceptualizarea totalității componentelor interfeței utilizator sistemului informatic, funcționalitățile sistemului informatic care cuprinde descrierea detaliată a totalității scenariilor de implementare a sistemului informatic. |
| **14** | Software Requirements Specification (SRS) | Document care conține descrierea detaliată a totalității scenariilor de interacțiune între utilizatori și aplicația informatică. |
| **15** | Bază de Date (BD) | Ansamblu de date organizate conform structurii conceptuale care descrie caracteristicele de bază și relația dintre entități |
| **16** | Veridicitatea datelor | Nivel de corespundere a datelor, păstrate în memoria calculatorului sau în documente, stării reale a obiectelor din domeniul respectiv al sistemului, reflectate de aceste date. |
| **17** | Scrutin | Alegerile în Parlament, pentru funcția de Președinte al Republicii Moldova, în autoritățile administrației publice locale, precum și referendumurile (de orice nivel). |
| **18** | Opțiune de votare | Lista concurenților electorali la Alegerile în Parlament, pentru funcția de Președinte al Republicii Moldova, în autoritățile administrației publice locale, precum și opțiunile la referendumuri. |
| **19** | Buletin electronic de vot | Document (electronic) cu care Alegătorul își exprimă opțiunea de votare. Documentul se emite pentru fiecare scrutin și circumscripție electorală și conține o listă de opțiuni de votare.<br>Alegătorul poate și trebuie să aleagă numai o opțiune de vot. |
| **20** | Ziua alegerilor | Ziua în care este stabilită efectuarea alegerilor. |

| | | |
|---|---|---|
| **21** | Observator extern | Utilizator care participă la procesul de observare a e-votării și dispune de totalitatea tranzacțiilor de e-votare descărcate din blockchain. |
| **22** | Vot electronic/e-vot/vot prin internet | Metoda de vot în care alegătorii își dau votul prin internet. |
| **23** | e-votant | Alegătorul, care și-a exprimat votul prin internet prin utilizarea SI e-Votare |
| **24** | e-vot exprimat | Vot al alegătorului depus prin Aplicația Alegătorului e-Votare criptat, semnat digital și transmis în Sistemul de Management e-Votare. |
| **25** | e-vot recurent | e-Vot exprimat de alegător de mai multe ori prin SI e-Votare. |
| **26** | e-vot dublu | e-Vot exprimat de alegător atât prin SI e-Votare, cât și prin secția de votare cu buletin de vot pe suport de hârtie. |
| **27** | HSM | Modul de securitate hardware și care este un procesor crypto sigur, axat pe furnizarea de chei criptografice și oferă, de asemenea, operațiuni criptografice accelerate cu ajutorul acestor chei. |
| **28** | Blockchain | Un registru digital descentralizat, distribuit și accesibil publicului, care înregistrează informații în așa fel încât orice înregistrare relevantă să nu poată fi modificată retroactiv fără a modifica toate blocurile ulterioare. |
| **29** | Nod | Nodul din rețeaua blockchain care procesează tranzacțiile, formează blocurile și implementează algoritmul de **consens**. |
| **30** | Consens | O modalitate prin care un grup de **participanți** poate ajunge la un rezultat convenit. |
| **31** | Participant | Participantul la blockchain care trimite **tranzacțiile** către rețea pentru confirmare. |
| **32** | Tranzacție | Transmiterea de "fapte" generate de participanții la o rețea pentru a iniția orice acțiune. |
| **33** | SmartContract | Algoritm informatic conceput pentru a genera, controla și furniza informații despre un acord între părți. |
| **34** | Criptare homomorfă | O formă de criptare care permite efectuarea anumitor operații matematice asupra textului cifrat și produce un rezultat criptat care corespunde rezultatului operațiilor efectuate asupra textului în clar. |
| **35** | Protecția criptografică a integrității datelor | Un mecanism de protecție prin criptarea datelor pentru stocarea sigură și protejarea informațiilor de utilizatorii nedoriți. |
| **36** | Cheia privată | O combinație de șiruri de caractere pentru semnarea tranzacțiilor și accesarea token-urilor, stocate în mod privat. Cheia privată este indisolubil legată de cheia publică. |
| **37** | Cheia publică | O combinație de șiruri de caractere legate indisolubil de cheia privată. Cheia publică este atașată tranzacțiilor pentru a verifica corectitudinea semnăturii utilizatorului făcută pe cheia privată. |
| **38** | Hash | O configurație unică de caractere (litere, numere) care rezultă în urma executării unei funcții hash pe date. Hash identifică în mod unic obiectul |
| **39** | Generarea distribuită a cheilor (DKG) | Un proces criptografic în care mai multe părți se angajează în calcularea unui set comun de chei publice și private. |

| | | |
|---|---|---|
| **40** | Protocolul de calcul multipartit (MPC) | Un protocol criptografic care permite mai multor părți să efectueze un calcul care depinde de datele secrete de intrare ale fiecărei părți, astfel încât nicio parte nu poate obține informații despre datele secrete de intrare ale celorlalți. |
| **41** | ZeroKnowledge Range Proofs | Un protocol criptografic interactiv care permite uneia dintre părțile care cooperează ("verificator") să asigure validitatea unei afirmații (de obicei matematice) fără nicio altă informație din partea celeilalte părți ("prover"). |

## 2.4 Obiectivele și destinația sistemului

Sistemul de vot prin internet are scopul de a oferi cetățenilor Republicii Moldova un instrument alternativ de vot, astfel ca procesul electoral să devină mai accesibil, incluziv, sigur și inovativ. Sistemul de vot prin internet este destinat tuturor alegătorilor Republicii Moldova, oriunde s-ar afla. Un obiectiv specific al votului prin internet îl reprezintă asigurarea accesului la procesul electoral pentru cetățenii aflați în dificultatea de a se deplasa la secția de votare.

## 2.5 Părțile implicate și rolul lor în sistemul informatic

Organizarea procesului electoral cu utilizarea votului prin internet depășește cadrul de responsabilitate exclusivă a Comisiei Electorale Centrale. Implicațiile tehnice și încadrarea în arhitectura TIC guvernamentală implică și alte instituții ce vor avea competențe în organizarea întregului proces de votare prin internet. Cele mai importante instituții în acest proces sunt:

1. Comisia Electorală Centrală, responsabilă de organizarea întregului proces electoral, atât în cadrul secțiilor de vot, cât și prin internet.
2. Serviciul Tehnologii Informaționale și Securitate Cibernetică, responsabil de asigurarea securității cibernetice și oferirea infrastructurii hardware pentru sistemul de vot prin internet, în perioada alegerilor.
3. Agenția pentru Servicii Publice, responsabilă de emiterea actelor de identitate, inclusiv a semnăturilor electronice pentru alegători, compatibilă cu mijloacele de autentificare în sistemul de vot prin internet, dar și de Registrul de stat al populației care participă în schimbul de date cu Registrul de stat al alegătorilor.
4. Serviciul de Informații și Securitate, responsabil de identificarea amenințărilor de securitate pentru procesul de vot prin internet, investigarea incidentelor de securitate aferente procesului electoral, stabilirea cerințelor tehnice pentru dispozitivele de creare a semnăturii electronice utilizate în cadrul procesului de vot prin internet.
5. Agenția pentru Guvernare Electronică, responsabilă de modernizarea serviciilor publice prin digitalizarea și reingineria lor, eficientizarea guvernării prin schimbul de date între autorități și instituțiile care prestează servicii publice, diversificarea canalelor de acces la serviciile publice și asigurarea securității informației.
6. Centrul Național de Protecție a Datelor cu Caracter Personal, responsabil de asigurarea protecţiei drepturilor şi libertăţilor fundamentale ale persoanei în ceea ce privește prelucrarea datelor cu caracter personal.

# 3 Principiile de elaborare SI e-Votare

Introducerea unor noi metode de exprimare a votului trebuie să respecte toate standardele existente, principiile participării la alegeri și cerințele pentru organizarea alegerilor în mod tradițional. Aceste principii sunt prevăzute de Constituție (sufragiu universal, egal, direct, secret și liber exprimat), de Codul electoral, dar și de tratatele internaționale la care Republica Moldova este parte.

Articolul 21 din Declarația Universală a Drepturilor Omului prevede elementele de bază ale dreptului la democrație și la alegeri democratice, menționând, în special, că "*[...] orice persoană are dreptul de a lua parte la administrarea treburilor publice ale țării sale, în mod direct sau prin reprezentanți liber aleși [...], și că voința poporului trebuie să constituie baza puterii de stat; această voință trebuie să fie exprimată prin alegeri nefalsificate, care sa aibă loc în mod periodic prin sufragiu universal, egal și exprimat prin vot secret sau urmând o procedură echivalentă care să asigure libertatea votului*". În același timp, Recomandarea Comitetului de Miniștri al Consiliului Europei (2004 și 2017) privind standardele juridice, operaționale și tehnice pentru votul electronic prezintă în Anexa I principiile electorale de bază și modul în care acestea trebuie să fie menținute în contextul procedurilor de vot prin internet.

Astfel, principiile participării la alegeri prin intermediul sistemului de vot prin internet sunt următoarele:

**Universalitatea votului** - Sistemul de vot prin internet trebuie să fie proiectat în așa fel, încât să sporească oportunitățile de participare la alegeri a persoanelor cu acces limitat. Votul prin internet trebuie să fie perceput drept o modalitate adițională de votare față de metoda tradițională unde alegătorul se prezintă fizic la secția de votare. În mod firesc, votul prin interent ar trebui să fie exercitată în oricare circumstanță, alegătorul având dreptul să aleagă o modalitate sau alta, în funcție de condițiile concrete în care se află. Condițiile pentru înregistrarea votului exprimat prin internet nu trebuie să reprezinte impedimente pentru participarea la alegeri.

**Egalitatea votului** – În cadrul alegerilor sau referendumului, alegătorii trebuie să introducă în urna virtuală (electronică) doar un singur vot valabil exprimat. Cu toate acestea, acest principiu nu trebuie confundat cu „vot multiplu – ultimul vot contează", concept care asigură unicitatea votului pe internet prin a-i permite alegătorului să voteze de mai multe ori, însă doar ultimul vot valabil exprimat să fie numărat. Acest principiu asigură și respectarea altor două principii de bază, precum: votul secret și libertatea de exprimare a votului. Mai mult decât atât, opțiunea de schimbare a votului ar putea fi un instrument eficient care ar evita vicierea votului. Astfel, faptul că alegătorul va putea să schimbe votul dat prin internet reduce interesul și motivația de a exercita orice influență sau presiune asupra alegătorului, inclusiv prin oferire de bani sau bunuri pentru exprimarea votului în favoarea unui anumit concurent electoral. În cazul în care un alegător alege să voteze din nou, după ce a votat deja prin internet, votul anterior este anulat și înlocuit cu votul final exprimat. Prin urmare, sistemul de vot prin internet funcționează în așa fel, încât să nu fie posibilă cuantificarea de două sau de mai multe ori a votului exprimat.

**Secretul votului** – Acest principiu presupune două dimensiuni. În primul rând, anonimatul alegătorului și, în al doilea rând, confidențialitatea de exprimare a votului. Anonimatul – votarea prin internet trebuie astfel organizată, încât să excludă orice posibilitate de a afecta confidențialitatea exprimării opțiunii de vot. În acest scop, voturile introduse on-line în urna virtuală trebuie să rămână anonime, iar numărul lor în niciun fel să nu facă referire la alegător. Astfel, organul electoral (CEC) este obligat să asigure că, pe perioada stabilirii rezultatului alegerilor, informațiile și datele utilizate să nu fie divulgate.

**Confidențialitatea** – Votul prin internet necesită, în primul rând, regândirea principiului confidențialității. Votarea în intimitate nu ar trebui să fie considerată un scop în sine. Votul exercitat în mod secret este, în același timp, un drept și o obligație a alegătorului. Dimensiunea de confidențialitate a secretului votului constă în protejarea alegătorului de orice presiune sau influență asupra exprimării libere a preferințelor sale politice. Astfel, alegătorul este obligat să se asigure că votul său a fost exprimat în condiții de confidențialitate și libere de orice presiune posibilă externă. În același timp, alegătorul trebuie să aibă libertatea de a alege modalitatea de a-și exprima votul, fie prin internet, fie cu prezență fizică la secția de votare prin intermediul buletinului de vot tipărit pe hârtie. Cu toate acestea, buletinul de vot tipărit pe hârtie rămâne a fi unul prioritar, deoarece votul electronic constituie doar un canal de vot adițional.

**Votul liber exprimat** – Modul de organizare a sistemului de vot prin internet trebuie să asigure atât formarea, cât și exprimarea, în mod liber, a opțiunilor de vot. Sistemul de vot prin internet trebuie să fie astfel conceput, încât alegătorii să nu își exprime opțiunea de vot în mod pripit și negândit. Alegătorul trebuie să aibă dreptul să își poată schimba opțiunea de vot oricând sau să poată întrerupe procedura votului prin internet, fără ca opțiunile anterioare să fie înregistrate. Sistemul nu va permite nicio influență manipulatoare asupra alegătorului în timpul votării. Sistemul trebuie să indice alegătorului, după exprimarea opțiunii de vot, că procedura a fost realizată și s-a finalizat cu succes. Sistemul de vot prin internet trebuie să prevină înregistrarea votului dublu. Astfel, așa cum s-a descris mai sus, în cazul votului multiplu doar ultimul va fi numărat, votul precedent exprimat fiind anulat în mod automat.

**Transparența procesului de votare prin internet** – organizarea și implementarea votului prin internet trebuie să fie astfel conceput, încât să asigure accesul tuturor părților interesate la toate informațiile și documentele (rapoartele) relevante procesului de vot.

Inovațiile ce însoțesc votul prin internet aduc și concepte noi care trebuie menționate:

**Canal alternativ de vot.** Votul prin internet nu înlocuiește votul fizic la secția de votare. Introducerea votului prin internet înseamnă că toate procedurile de vot vor rămân funcționale. Alegătorilor li se oferă un canal auxiliar de vot ca o alternativă viabilă și sigură.

**Votul prin internet anticipat.** Toate sistemele de vot prin internet, în cazul în care sunt utilizate în calitate de canal alternativ de vot, sunt disponibile pentru utilizare înainte de ziua efectivă a alegerilor, adică în prealabil, de regulă, timp de 2 – 4 zile, de exemplu, de luni pană joi înainte de ziua alegerilor (Duminică). Acest lucru este necesar din două considerente. Primul, este permisă exercitarea votului prin internet de mai multe ori, însă doar ultima opțiune de vot este cea valabila; al doilea, există timp suficient pentru a marca în listele electorale toți alegătorii care au votat prin internet, astfel încât să fie păstrată unicitatea votului, adică alegătorul să nu poată vota prin intermediul buletinului de vot tipărit pe hârtie, dacă nu a fost radiat buletinul electronic din urna electronică. De asemenea, perioada între ziua alegerilor și ultima zi pentru votarea prin internet este dedicată analizei integrității datelor și a sistemului, pentru a identifica posibile intervenții neautorizate și dacă au fost respectate toate procedurile tehnice și de securitate cibernetică. În cazul depistării unor intervenții neautorizate și a constatării faptului că datele sau sistemul au fost compromise, alegătorul va fi invitat să voteze în cadrul secției de vot (off-line) în ziua alegerilor.

**Votul multiplu prin internet (ultimul vot fiind cel valabil).** – Prioritate se dă votului exercitat în baza buletinului de vot tipărit pe hârtie. După cum s-a menționat deja, votarea multiplă prin internet nu înseamnă cuantificarea aceluiași vot de mai multe ori, operațiune care, în toate cazurile, se consideră o încălcare a principiului egalității votului. De fapt, acest concept înseamnă că un alegător care dorește să voteze prin internet o poate face de mai multe ori în perioada fixată pentru votarea anticipată, fiind numărat doar ultimul vot. Aceasta este considerată a fi o măsură eficientă de prevenire a influenței altor persoane

asupra alegătorului. Mai mult, conceptul de vot multiplu prin internet implică, de asemenea, un alt concept, și anume: prioritatea votului exprimat prin intermediul buletinului de vot tipărit pe hârtie. Astfel, sistemul de vot prin internet este doar un canal alternativ modului tradițional de exprimare a votului, iar dreptul alegătorului de a-și exercita votul prin intermediul buletinului de vot tipărit pe hârtie în ziua alegerilor trebuie să fie garantat, chiar și în cazul în care alegătorul și-a exprimat deja un vot prin internet. Astfel, votul final exprimat prin intermediul buletinului de vot tipărit pe hârtie trebuie considerat valabil și prioritar, iar votul electronic anterior exprimat trebuie anulat în mod automat de către sistemul de vot prin internet.

**Votul la distanță într-un "mediu neformal".** Actualmente, sistemul electoral din Republica Moldova recunoaște doar votul exprimat într-un "mediu controlat", adică votul exprimat la o secție de votare desemnată, unde este asigurat caracterul de confidențialitate al procesului de către membrii biroului electoral al secției de votare. Votul la distanță prin internet reprezintă votarea într-un "mediu necontrolat", adică de acasă sau din orice altă locație unde există acces la internet.

Similitudinea dintre votarea prin internet și votul obișnuit sunt evidente, întrucât ambele sisteme trebuie să respecte aceleași principii. Votarea prin internet se racordează prevederilor, principiilor și bunelor practici în domeniul electoral. Prin urmare, acesta este uniform și secret, exprimat de toți cetățenii cu drept de vot. Procesarea voturilor este securizată și sigură. Alegătorul trebuie să aibă posibilitatea de a-și exprima votul liber, fără a fi impus sau influențat din exterior. Este interzisă determinarea participării la votare prin internet prin a-i pune la dispoziție alegătorului un calculator sau un dispozitiv în acest scop ori influențându-l prin orice alt mod, de asemenea este interzisă organizarea întrunirilor de votare prin internet în mod colectiv (deschiderea oficiilor sau a birourilor de servicii pentru votarea prin internet etc.), deoarece astfel de activități pot fi interpretate drept încălcare a votului liber exprimat. Un alegător poate vota doar pentru sine însuși. Nu se permite utilizarea actelor de identitate în scop de a vota de către netitularii acestora.

# 4 Actorii sistemului

Actorii implicați în procesele business din cadrul componentelor sistemului SI e-Votare și descrierea acestora sunt prezentate în tabelul de mai jos:

| ID | Actor | Descriere actor |
|---|---|---|
| **1** | Alegător | Actor uman, care utilizează aplicația mobilă e-Votare destinate exercitării dreptului de vot electronic la distanță. |
| **2** | Organizator | Actor uman cu acces la funcționalitățile SI e-Votare legate de procesul de organizare a alegerilor și administrare a proceselor de e-votare. |
| **3** | Membru CEE | Actor uman cu acces la funcționalitățile SI e-Votare aprobare a totalizărilor legate de procesare și numărare a e-voturilor exprimate. |
| **4** | Colector | Actor nonuman responsabil de derularea serviciilor dedicate din cadrul Componentei Colector din Sistemului de Management e-Votare. |
| **5** | Procesator | Actor nonuman responsabil de derularea serviciilor dedicate din cadrul Componentei Procesator din Sistemului de Management e-Votare. |
| **6** | Contor | Actor nonuman responsabil de derularea serviciilor dedicate din cadrul Componentei Contor din Sistemul de Management e-Votare. |
| **7** | Observator extern | Actor uman responsabil de monitorizare date privind e-voturile exprimate în scop de audit extern. |
| **8** | Sistem | Actor nonuman responsabil de jurnalizare evenimente din cadrul Componentei Contor din Sistemului de Management e-Votare. |

Mai jos este prezentată descrierea detaliată a actorilor umani din cadrul SI e-Votare și a accesului acestora la funcționalitățile sistemului.

**Alegător** - reprezintă utilizator cu acces la funcționalitățile Aplicației Alegătorului e-Votare destinate exercitării dreptului de vot prin utilizarea internetului. Aplicația Alegătorului trebuie să dispună de următoarele funcționalități:

1. Autentificare alegător
2. Încărcare și afișare date necesare exercitării votului electronic
3. Exercitarea votului electronic la distanță în intervalul de timp disponibil votării
4. Modificarea opțiunii de vot în intervalul de timp disponibil votării

Este necesar de remarcat, că alegătorul trebuie să poată să-și modifice opțiunea de vot electronic pe parcursul perioadei de e-votare. Valabilă trebuie să fie considerat numai ultima opțiune de e-vot. Mai mult, alegătorul poate vota și la secțiile de votare. În acest caz, trebuie să se numere doar votul exprimat în buletinul de vot pe suport de hârtie, iar e-votul exprimat de alegător trebuie să fie anulat. Acest principiu îi protejează și pe alegători împotriva constrângerii.

**Organizator** este utilizator autorizat care dispun de acces la funcționalitățile necesare declanșării procesului de setare a e-votării. Utilizatorii trebuie să dispună de acces la funcționalitățile Sistemului de Management e-Votare. Aceste funcționalități sunt:

1. Import date pre-alegeri
    a. liste scrutine, circumscripții electorale, opțiuni de votare
    b. liste alegători
2. Lansarea și oprirea procesului de la diverse etape din componentele Sistemului de Management e-Votare
    a. e-votare
    b. de procesare e-voturi
    c. de numărare e-voturi
3. Import/export date din Componentele Sistemului de Management e-Votare.
4. Îndeplinire activități de administrare SI e-Votare
    a. definirea politicilor de acces la sistem și componentele acestuia
    b. monitorizarea procesului de vot
    c. monitorizarea proceselor de securitate a SI e-Votare.

**Membru CEE** este utilizator autorizat deținător de parte a cheii private de decriptare rezultat numărare e-voturi exprimate și anonimizate. Membrul CEE va semna digital procesele verbale pe parcursul procesării și rezultatele numărării e-voturilor exprimate.

**Observator extern** este actor uman cu acces la responsabil de monitorizare date privind e-voturile exprimate în scop de audit extern.

# 5 Arhitectura SI e-Votare

Din punct de vedere instituțional, SI e-Votare reprezintă un complex de resurse informaționale integrate în SIASA și destinate să asigure procesul de votare prin internet.

Locul SI e-Votare în infrastructura TIC a CEC și infrastructura guvernamentală este prezentat în diagrama din Figura 1.

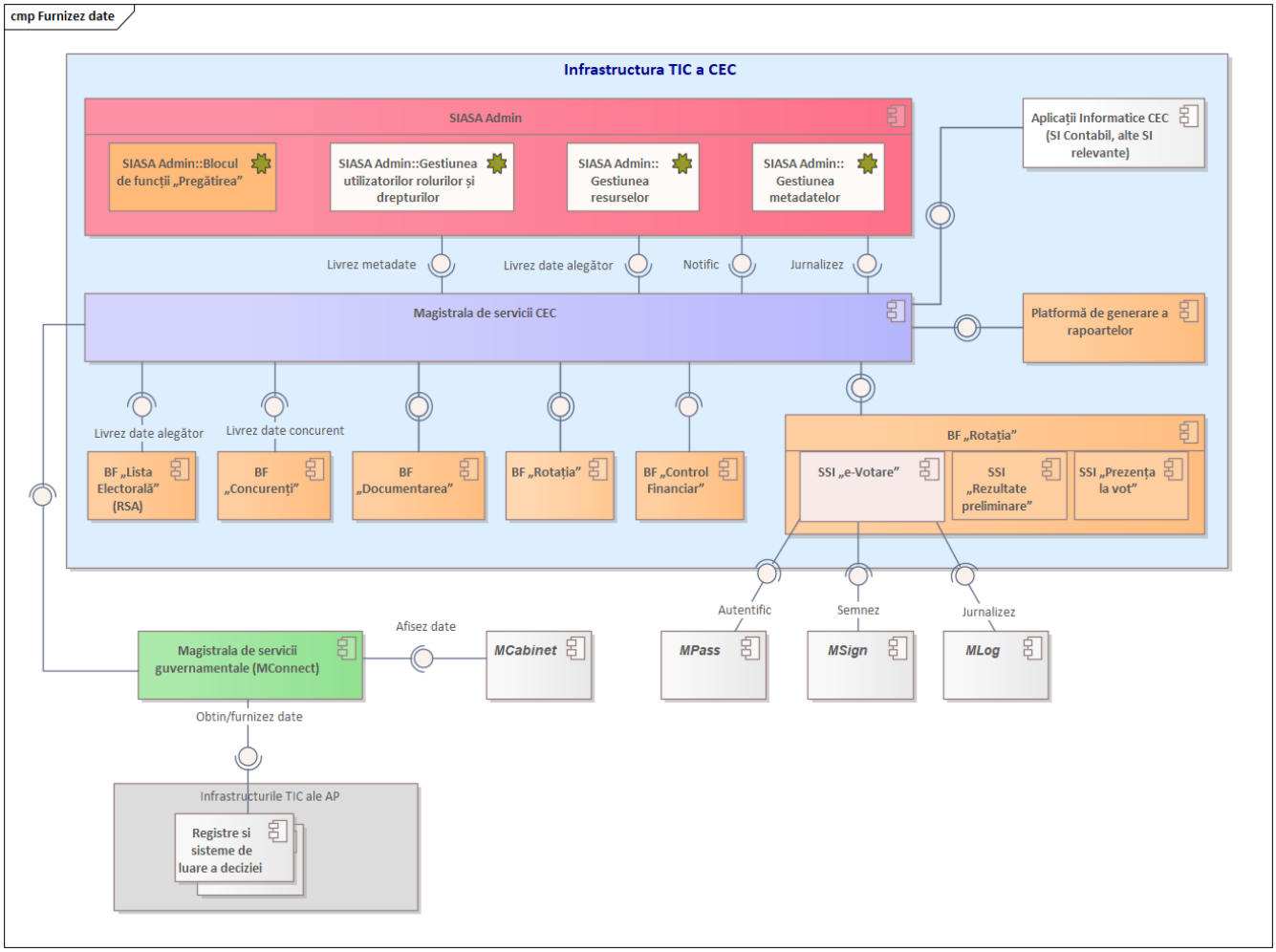



Figura 1. Locul SI e-Votare în infrastructura TIC a CEC și infrastructura guvernamentală.

SI e-Votare este conceput ca un sistem informațional, care va interacționa cu mai multe sisteme și subsisteme (blocuri funcționale) atât din cadrul CEC-ului, cât și la nivel guvernamental cu sistemele informaționale ale altor autorități publice centrale ale Republicii Moldova. În acest sens este oportună utilizarea cadrului de interoperabilitate a Guvernului pentru realizarea conexiunilor cu sisteme informatice terțe sau utilizarea serviciilor de platformă furnizate de acesta.

SI e-Votare este conceput ca un complex de aplicații și sisteme (cu mai multe componente) care interacționează între ele și este compus din:

- Aplicația Alegătorului e-Votare
- Sistem de Management e-Votare
- Sistem de Observare e-Votare.

SI e-Votare trebuie să dispună de mecanisme de interoperabilitate cu următoare sisteme și servicii externe:

- SIASA Admin
- RSA
- SI Ziua Votului (SI EDay)
- Serviciile MPass și MSign.

Mai jos sunt prezentate descrierile acestor aplicații, sisteme și a Componentelor SI e-Votare.

**Aplicația Alegătorului e-Votare** este destinată alegătorului și va rula pe dispozitivul mobil al alegătorului. Această aplicație va permite alegătorului să-și exprime votul.

Aplicația Alegătorului prin intermediul unei componente de backend va comunica atât cu alte sisteme și servicii externe, cât și cu Sistemul de Management e-Votare.

Componenta Backend pentru Aplicația Alegătorului e-Votare (Web API) este concepută ca un set de servicii (API-uri):

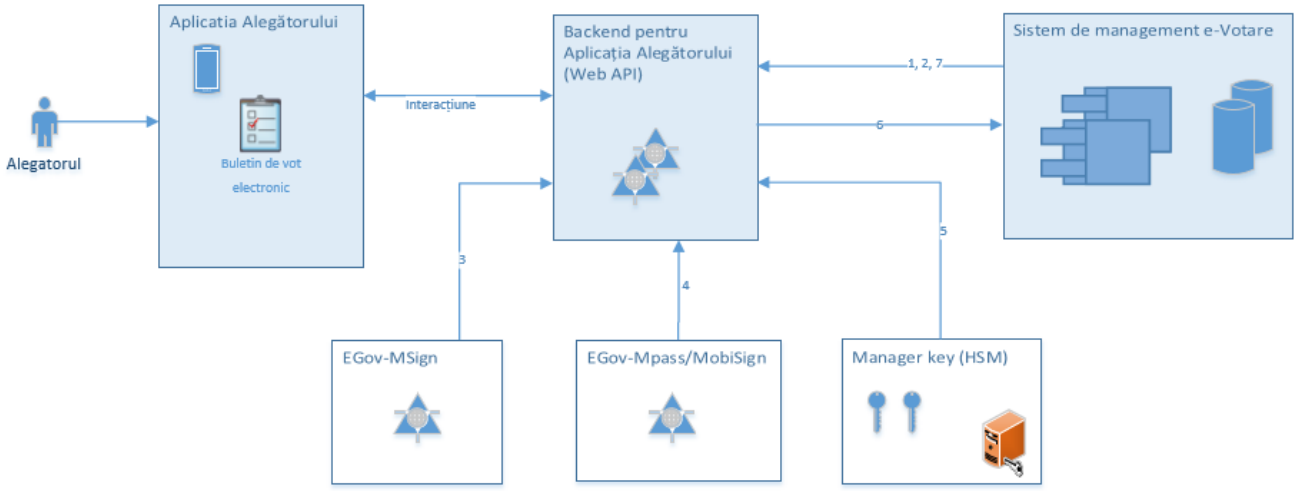
- serviciul integrare cu serviciul guvernamental de autentificare MPass – în scop de identificare și autentificare
- serviciul integrare cu serviciul guvernamental de semnare electronică MSign – pentru semnare digitală buletin de vot electronic
- serviciu de import din Sistemul de Management e-Votare date necesare procesului de e-votare:
    - date alegător
    - scrutine din ziua alegerilor
    - circumscripții electorale la care este arondat alegătorul pentru scrutinele din ziua alegerilor
    - opțiunile de votare din buletinele de vot
    - metadate aferente buletinelor de vot
- serviciu de încărcare date aferent cheii publice în scop de criptare voturi
- serviciu de integrare cu Sistemul de Management e-Votare în privința e-votării (transmitere e-vot exprimat, recepționare mesaje, cod de verificare, etc).

Datele alegătorului și datele aferente scrutinelor/circumscripțiilor/buletinelor se vor stoca în aplicația alegătorului și vor forma buletinele de vot electronice cu opțiuni de votare.

După confirmarea, criptare și semnarea electronică a voturilor exprimate datele alegătorului și a voturilor exprimate se vor transmite în Sistemul de Management e-Votare, utilizând metoda dublului plic (plicul extern identifică alegătorul, iar plicul intern conține votul exprimat, criptat).

De asemenea, Aplicația Alegătorului e-Votare va recepționa și afișa un cod pe baza căruia Alegătorul poate verifica dacă e-votul exprimat a ajuns corect în componenta ”Colector” din Sistemul de Management e-Votare și dacă e-votul stocat este e-votul exprimat.

În Figura 2 este prezentat locul Aplicației Alegătorului e-Votare în SI e-Votare și modul de interacțiune cu alte sisteme și servicii externe și cu Sistemul de Management e-Votare.




1. Date alegător
2. Date buletine de vot (scrutin, circumscripția, opțiuni de votare)
3. Certificatul cheii publice (pentru semnare vot exprimat)
4. Certificatul cheii publice (pentru autentificare)
5. Certificatul cheii publice (pentru criptare vot exprimat)
6. Vot exprimat (criptat și semnat)
7. Identificator unic a votului exprimat

Figura 2. Aplicația Alegătorului e-Votare și interacțiunea cu alte sisteme, aplicații și servicii.

Sistem de Management e-Votare este destinat stocării, procesării și numărării e-voturilor exprimate și trebuie să conțină următoarele componente:

- Componenta “Colector”, care include o subcomponentă ”Registrator”
- Componenta “Procesator”
- Componenta ”Contor”
- Componenta “Audit”
- Componenta “Interfață utilizator”

**Componenta “Colector”** din Sistemul de Management e-Votare are destinația de colectare și stocare e-voturilor exprimate. De asemenea, componenta trebuie să dispună de o **subcomponentă “Registrator”** de comunicare cu sistemele și aplicațiile și serviciile atât din SI e-Votare, cât și externe.

**Subcomponenta “Registrator”** din Sistemul de Management e-Votare trebuie să dispună de :

- Interfață de acces la instrumentele și serviciile subcomponentei.
- Servicii de import date din infrastructura TI a CEC-ului a următoarelor informații:
  - Lista scrutine din ziua alegerilor
  - Lista circumscripții electorale per fiecare scrutin

    - Lista opțiuni de votare per fiecare circumscripție
    - Lista secții de votare
    - Metadate aferente buletinelor de vot
    - Lista alegătorilor eligibili la scrutinele din ziua alegerilor.
- Servicii de transmitere în aplicația alegătorului e-Votare a următoarelor informații:
    - date personale a alegătorilor
    - date despre scrutine din ziua alegerilor, circumscripții electorale la care este arondat alegătorul pentru scrutinele din ziua alegerilor.
- Servicii de recepționare (prin intermediul componentei de backend a aplicației alegătorului e-Votare) și transmitere pentru stocare în Componenta ”Colector” a informației:
    - date e-votant
    - date buletine de vot electronice cu voturile exprimate criptate și semnate electronic.

**Componenta “Colector”** din Sistemul de Management e-Votare trebuie să dispună de:

- Interfață de acces la instrumentele și serviciile componentei.
- Serviciu de stocare informații recepționate din Componenta ”Registrator”:
    - date e-votant
    - date buletine de vot electronice cu voturile exprimate criptate și semnate electronic.
- Serviciu de export date e-votanți și e-voturi exprimate către Componenta ”Procesator” și SI Ziua votului.
- Serviciu de transmitere hash e-voturi exprimate în blockchain.

**Componenta “Procesator”** din Sistemul de Management e-Votare are destinația de procesare e-voturi exprimate. Componenta trebuie să dispună de:

- Interfață de acces la instrumentele și serviciile componentei.
- Serviciu de import date din componenta ”Colector”.
- Serviciu de import date din SI Ziua Votului despre votanți în Secțiile de Votare.
- Serviciu de verificare integritate e-voturi exprimate.
- Serviciu de anulare e-voturi recurente (va rămâne valabil doar ultimul e-vot exprimat).
- Serviciu de anulare e-voturi duble (va rămâne doar votul exprimat la secția de votare prin buletine de vot pe suport de hârtie)
- Serviciu de anonimizare voturi
- Serviciu de export date voturi pentru numărare în componenta ”Contor”

**Important!** Serviciu de anulare e-voturi duble poate fi lansat numai după finalizare votare în secțiile de votare. Atenție – Secțiile de votare de peste hotare se închid după ora locală a secției.

**Componenta ”Contor”** din Sistemul de Management e-Votare are destinația de numărare e-voturi exprimate și criptate. Componenta trebuie să dispună de:

- Interfață de acces la instrumentele și serviciile componentei.
- Serviciu de import date e-voturi exprimate și procesate din componenta ”Procesator”
- Serviciu de numărare e-voturi exprimate și criptate
- Serviciu de export rezultat numărare e-votare criptate.

În Figura 3 este prezentat locul Sistemul de Management e-Votare în SI e-Votare și modul de interacțiune cu alte aplicații/sisteme și servicii (inclusiv externe).

**Componenta "Interfața utilizator"** este destinată accesării de către utilizatori autorizați a diverselor servicii și instrumente necesare pentru funcționarea componentelor sistemului. Printre acestea trebuie de menționat:

- setarea parametrilor de funcționare a sistemului (perioadă e-votare, etc)
- înregistrare membri CEE - deținători de părți de cheie privată de decriptare rezultat numărare e-voturi
- alte instrumente și servicii identificate la etapa de proiectare sistem.

**Componenta "Audit"** este destinată jurnalizării evenimentelor produse în cadrul Sistemului de Management e-Votare.

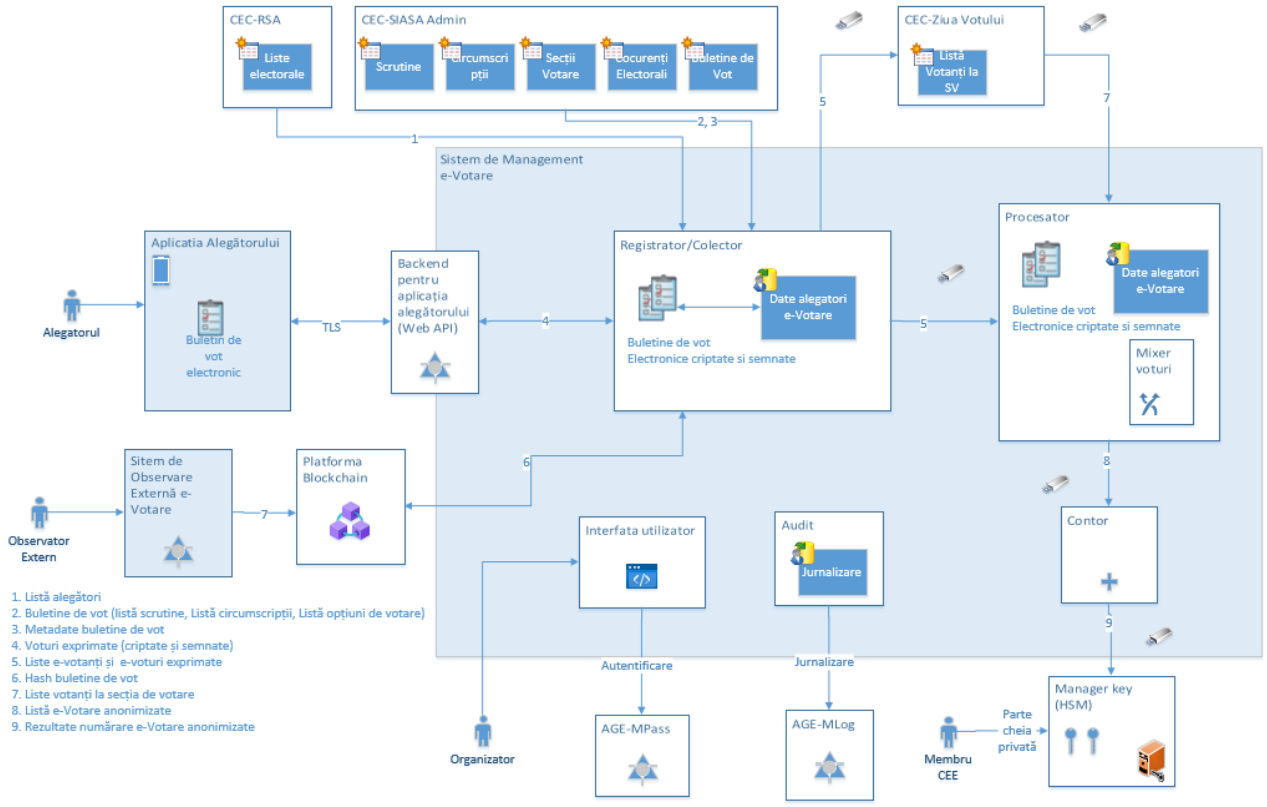



Figura 3. Sistemul de Management e-Votare și interacțiunea cu alte aplicații, steme și servicii.

**Sistemul de Observare e-Votare** este destinată observatorului extern și va fi implementată ca o pagina Web . Această aplicație va permite observatorului extern să monitorizeze mersul e-votării. Pentru acesta el trebuie să dispună de instrumente și servicii dedicate:

- serviciu de import/ din Sistemul de Management e-Votare date privind e-voturi anonimizate.

- serviciu de acces la date stocate în blockchain.

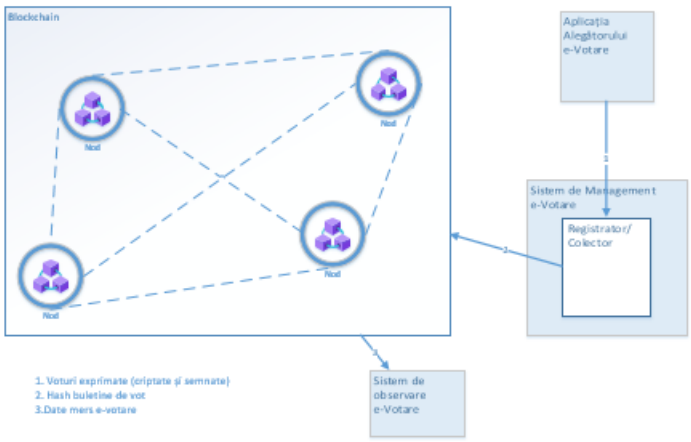



Figura 4. Sistemul de Observare e-Votare și interacțiunea cu alte sisteme, aplicații și servicii.

**Notă.** În domeniul votării prin internet, tehnologia registrelor distribuite își demonstrează cel mai clar avantajele - în primul rând, transparența și securitatea. Astfel, folosind proprietățile rețelei blockchain, algoritmi criptografici moderni (inclusiv criptografia homomorfică), partajarea cheilor de criptare este posibil de dezvoltat un sistem informațional de votare prin internet cu ajutorul căreia se poate organiza un proces de votare de încredere.

# 6 Etapele votării de la distanță

Scrutinele din ziua alegerilor dispun de următoarele etape:

- Pre-alegeri
- Votarea
- Numărarea voturilor
- Anunțarea rezultatelor alegerilor

SI e-Votare este o parte componentă a procesului de votare, care asigură votare de la distanță prin internet. Astfel, aceste procese sunt valabile și pentru votarea prin internet. Dar pentru asigurarea e-votării este necesar de întreprins și acțiuni suplimentare.

## 6.1 Etapa pregătire alegeri

În timpul **etapei pre-alegeri** SI e-Votare trebuie să fie setat cu următoarele:

- listele scrutinelor din ziua alegerilor
- listele circumscripțiilor electorale per fiecare scrutin
- listele opțiunilor de votare (de concurenți electorali pentru alegeri președinte/parlament/locale și/ori opțiuni pentru referendum) per fiecare circumscripție
- listele secțiilor de votare
- listele alegătorilor eligibili de participare la scrutine
- pentru fiecare scrutin sunt create chei publice și private pentru criptare și decriptare voturi
- aplicația alegătorului pentru votare
- aplicația alegătorului de verificare a votului exprimat
- instrucțiunile relevante aplicațiilor alegătorului sunt publicate.
- datele necesare pentru verificarea autenticității și integrității aplicațiilor alegătorului sunt publicate.

Trebuie să fie implementate următoarele proceduri de control pre-alegeri:

- Informațiile electorale folosite de platforma e-votare în timpul votării și numărării voturilor trebuie să fie controlabile în vederea detectării oricărei încercări de manipulare. Sunt considerate a fi electorale acele informații în format electronic care sunt utilizate de platforma de vot sau de observatori pentru a verifica configurația corectă a alegerilor. Acestea includ conținutul listelor electorale, mostrele buletinelor de vot, etc.
- Mai mult, componentele diferite ale softului pentru platforma de vot trebuie să fie certificate pentru a detecta orice tentativă de imixtiune. Acest fapt trebuie să le ajute observatorilor și alegătorilor să verifice dacă componentele utilizate sunt similare celor supuse controlului.
- Sistemul trebuie să verifice dacă informațiile electorale sunt certificate de CEC înainte de lansare a procesului de votare și de numărare a voturilor.
- Sistemul trebuie să permită observatorilor să verifice dacă informațiile electorale folosite de platforma de vot au fost certificate adecvat de CEC.

- Se recomandă ca sistemul să verifice integritatea configurării alegerilor și că această configurare permite funcționarea corectă a sistemului.
- Alegătorii trebuie să aibă capacitatea de a verifica integritatea și autenticitatea oricărei componente de vot executat pe terminalul lor de vot înainte de a-l închide (de ex., verificarea semnăturii digitale de pe aplicația de vot).

## 6.2 Votarea

Alegătorul va utiliza o Aplicație (Aplicația Alegătorului e-Votare). Procesul de votare de la această etapă va include următorii pași:

1. Alegătorul trebuie să descarce Aplicația Alegătorului.
2. Alegătorul trebuie să se autentifice în aplicație cu utilizarea serviciului guvernamental MPass.
3. Aplicația Alegătorului trebuie să solicite datele relevante din Sistemul de Management e-Votare.
4. În Sistemul de Management e-Votare trebuie să se verifice disponibilitatea de date solicitate pentru alegător și să se returneze datele.
5. Alegătorul î-și exprimă opțiunile de votare.
6. Aplicația Alegătorului trebuie să genereze un buletin de vot electronic pentru opțiunea exprimată criptat cu cheia publică a alegerilor. Un număr aleatoriu generat de Aplicația Alegătorului trebuie să fie, de asemenea, utilizat la criptare.
7. Aplicația Alegătorului trebuie să solicite alegătorului să semneze digital buletinul de vot criptat și datele alegătorului cu utilizarea serviciului guvernamental MSign.
8. Aplicația Alegătorului trebuie să trimită buletinul de vot criptat și datele alegătorului semnate digital în Sistemul de Management e-Votare.
9. Aplicația Alegătorului trebuie să returneze un cod unic al votului în scop de verificare ulterioară a e-votului exprimat.

În diagrama din  Figura 5 de mai jos este prezentată transmiterea e-votului exprimat.


Figura 5. Transmiterea e-votului exprimat.

Votul prin internet urmează structura dublului plic, când alegătorul creează în timpul procedurilor de vot un plic interior (care este în esență un vot criptat) și un plic exterior (care este în esență o semnătură digitală). Schema plicurilor digitale duble este prezentată în Figura 6.

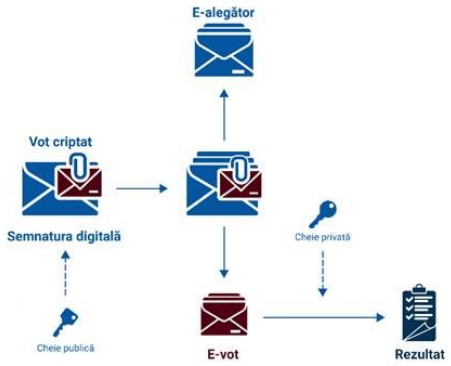



Figura 6. Structura plicurilor digitale duble.

## 6.3 Stocare, Procesare și Numărare voturi

Stocarea, procesarea și numărarea e-voturilor exprimate se va face în Sistemul de Management e-Votare. Acest proces va include următoarele activități:

1. Registratorul va primi din aplicația alegătorului e-votul criptat și semnat.
2. Registratorul va verifica validitatea certificatului utilizat pentru semnare. Dacă certificatul este valabil, acesta oferă o confirmare a valabilității și îl va transmite către Colector.
3. Dacă certificatul sau semnătura sunt invalide, atunci Registratorul va respinge buletinul de vot. Evenimentul de respingere este jurnalizat.
4. Colectorul va primi de la Registrator e-votul criptat și valabil semnat, va aplica marcajul de timp și va stoca buletinul de vot criptat semnat. De asemenea, se vor stoca datele alegătorului (inclusiv hash-ul), iar evenimentul se va jurnaliza.
5. După finalizarea e-votării, din Colector e-voturile se vor transmite la Procesator.
6. Procesatorul verifică integritatea e-votului exprimat (valabilitatea semnături digitale, marcajul de timp aplicat).
7. Procesatorul verifică dacă alegătorul a votat deja prin internet.
8. Dacă alegătorul a votat deja, atunci Procesatorul mută buletinului de vot anterior într-un jurnal, șterge buletinul anterior și jurnalizează evenimentul.
9. La încheierea acestei etape, Procesatorul va emite liste de e-votanți către secțiile de votare.
10. După finalizarea votării la secțiile de votare, în Procesator se încarcă listele de voturi exprimate la secțiile de votare.
11. Dacă alegătorul a votat la secția de votare, atunci se anulează votul prin internet. Procesatorul mută buletinul de vot electronic într-un jurnal, șterge buletinul și jurnalizează evenimentul.
12. Procesatorul grupează toate buletinele de vot electronice în funcție scrutin și de circumscripții electorale.
13. Procesatorul separă datele alegătorului (inclusiv cu semnăturile digitale), stocând aceste date ca o dovadă a cine a votat de datele votului exprimat și criptat.
14. Buletinele de vot criptate fără semnături sunt apoi exportate pe suporturi fizice și transferate la Contor pentru a fi numărate.

15. Contorul acceptă, prin intermediul suporturilor fizice, lista buletinelor de vot criptate sortate pe scrutine și circumscripții.
16. Contorul (pentru fiecare scrutin și circumscripție) numără e-voturile criptate (fără a fi decriptate cu utilizarea algoritmilor din criptarea homomorfică) și descarcă rezultatul numărării e-voturilor exprimate anonimizate.
17. Rezultatul numărării e-voturilor exprimate anonimizate se încarcă în HSM.
18. Un număr minim suficient de Membri CEE inserează criptostick-uri cu interfețe USB în dispozitiv HSM și decriptează rezultatele numărării e-voturilor exprimate.

## 6.4 Anunțarea rezultatelor alegerilor

Rezultatele e-votării peste care este aplicată semnătura digitală a Membrilor CEE sunt descărcate numărate și transmise la CEC pentru totalizare.

# 7 Cazurile de utilizare și cerințele funcționale aferente

În diagramele de mai jos sunt prezentate cazurile de utilizare executate de actorii sistemului.

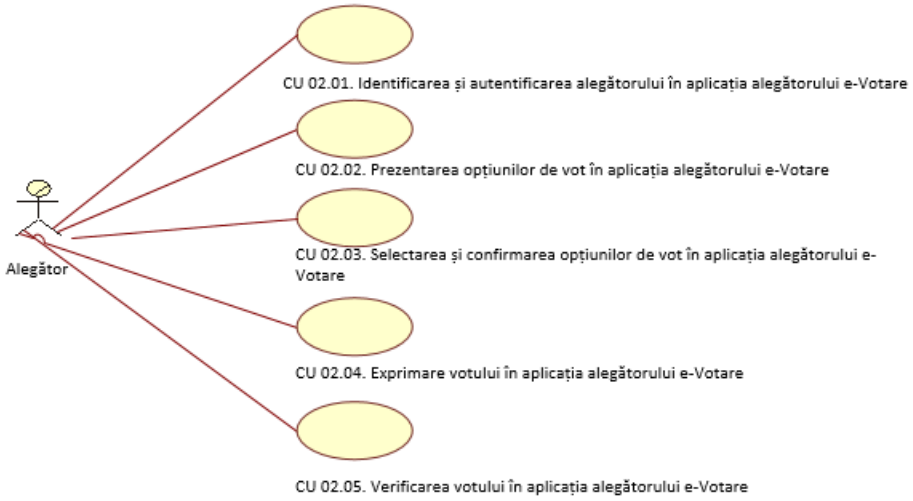



Figura 7. Diagrama cazurilor de utilizare aferent Aplicației Alegătorului.

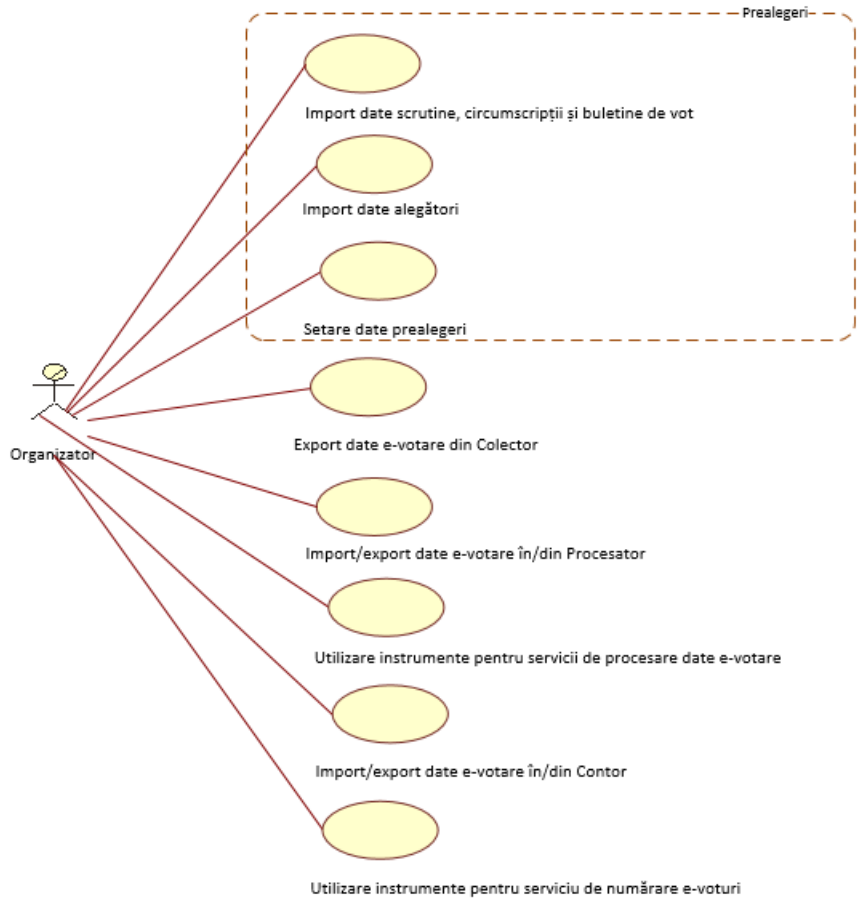
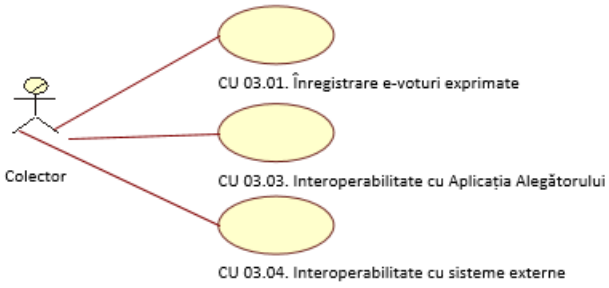



Figura 8. Diagrama cazurilor de utilizare aferent actorului cu rol ”Organizator”.



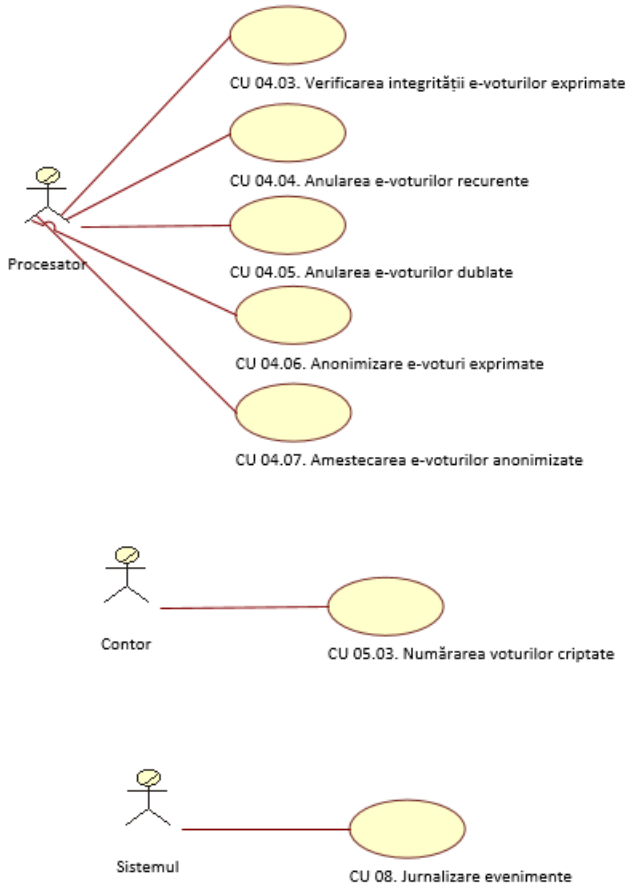
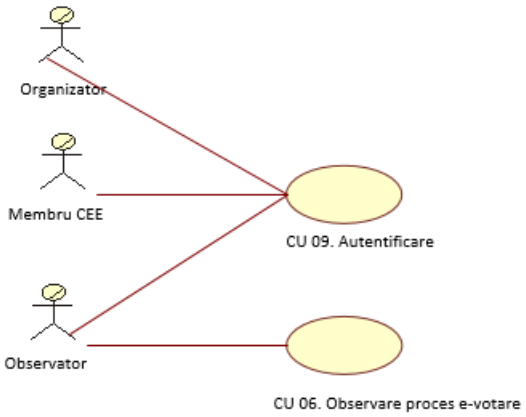



Figura 9. Diagramele cazurilor de utilizare aferent Actorilor nonumani.



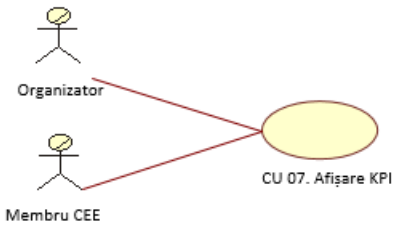



Figura 10. Diagramele altor cazurilor de utilizare.

Descrierea cazurilor de utilizare și cerințele funcționale aferente sunt prezentate în următoarele compartimente.

## 7.1 Cazuri de utilizare prealegeri

În acest compartiment sunt prezentate cerințele funcționale pentru cazurile de utilizare legate de activități de pregătire  pentru cotare prin internet. Componenta este destinată

- importului și stocării de date prealegeri
- setări informații prealegeri.

### 7.1.1 CU 01.01. Import date scrutine, circumscripții și buletine de vot

Cazul de utilizare este destinat importului și stocării de date din infrastructura TI a CEC-ului legate de gestiune scrutine, circumscripții electoral și opțiuni de votare.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.1.1.1** | Obligatorie | Sistemul trebuie să dispună de capabilitatea de organizare desfășurare paralelă a mai multor scrutine într-o zi de alegeri (fiecare scrutin va dispune de organizare individuală a circumscripțiilor electorale). |
| **7.1.1.2** | Obligatorie | Sistemul trebuie să dispună de **interfață** care asigură gestionarea proceselor de import date electorale. |
| **7.1.1.3** | Obligatorie | Sistemul trebuie să dispună de serviciu de import din SIASA date electorale necesare derulării procesului de votare:<br>- Lista scrutinelor din ziua alegerilor<br>- Lista circumscripții electorale pentru fiecare scrutin<br>- Lista opțiuni de votare pentru fiecare circumscripție electorală<br>- Lista secțiilor de votare. |

| | | |
|---|---|---|
| **7.1.1.4** | Obligatorie | Sistemul trebuie să dispună de serviciu de import din SIASA metadate aferent buletinelor de vot (simbolul electoral, ordinea amplasării concurenților electorali în buletin, alte date relevante). |
| **7.1.1.5** | Obligatorie | Sistemul trebuie să dispună de structură de stocare date electorale importate. |
| **7.1.1.6** | Obligatorie | Datele importate trebuie să dispună de identificatori unici și de proprietăți suficiente pentru asigurarea procesului de e-votare. |
| **7.1.1.7** | Obligatorie | Structura datelor destinate importului/exportului se va determina la etapa de dezvoltare a sistemului. |
| **7.1.1.8** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de operațiuni de import/export din cadrul componentei. |
| **7.1.1.9** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de import/export date. |
| **7.1.1.10** | Obligatorie | Serviciile de import sunt accesate de către Organizator. |

### 7.1.2 CU 01.02. Import date alegători

Cazul de utilizare este destinat importului și stocării de date din infrastructura TI a CEC-ului legate de listele electorale.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.1.2.1** | Obligatorie | Sistemul trebuie să dispună de interfață care asigură gestionarea proceselor de import liste electorale. |
| **7.1.2.2** | Obligatorie | Sistemul trebuie să dispună de serviciu de import din SIASA și de stocare date privind listele electorale necesare derulării procesului de votare (cel puțin următoarele date: IDNP, Nume, Prenume, Sexul, Data nașterii, Date adresă, Secția de Votare). |
| **7.1.2.3** | Obligatorie | Datele importate trebuie să dispună de identificatori unici și de proprietăți suficiente pentru asigurarea procesului de e-votare. |
| **7.1.2.4** | Obligatorie | Structura datelor destinate importului se va determina la etapa de dezvoltare a sistemului. |
| **7.1.2.5** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de operațiuni de import/export din cadrul componentei. |
| **7.1.2.6** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de import/export date. |
| **7.1.2.7** | Obligatorie | Serviciile de import sunt accesate de către Organizator. |

### 7.1.3 CU 01.03. Setare date prealegeri

Cazul de utilizare este destinat prezentării de instrumente și interfețe de care trebuie să dispună sistemul de e-votare utilizate pentru pregătirea votării prin internet.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.1.3.1** | Obligatorie | Sistemul trebuie să dispună de interfață și de instrumente de setare valori a parametrilor de funcționare a sistemului de e-votare. |
| **7.1.3.2** | Obligatorie | Sistemul trebuie să dispună de interfață de setare a valorilor parametrilor de funcționare a sistemului:<br>-Lista membrilor CEE (Nume, Prenume, IDNP)<br>-Număr total de chei de acces necesar pentru decriptare<br>-Număr minim de chei de acces necesar pentru decriptare<br>-Perioada e-votare (Data și ora început e-votare și Data și ora sfârșit e-votare (ora Moldovei))<br>-Perioada de timp pentru votarea repetată<br>-Perioada de timp pentru verificarea votului exprimat. |
| **7.1.3.3** | Obligatorie | Sistemul trebuie să dispună de interfață și instrumente de definire și configurare noduri blockchain. |
| **7.1.3.4** | Obligatorie | Sistemul trebuie să dispună de interfață și instrumente de definire și configurare date legate de cheia publică . |
| **7.1.3.5** | Obligatorie | Sistemul trebuie să dispună de interfață și instrumente de definire date de autenticitate și integritate a Aplicației Alegătorului. |

## 7.2 Cazuri de utilizare a Aplicației Alegătorului

În acest compartiment sunt prezentate cerințele funcționale pentru cazurile de utilizare ale Aplicației Alegătorului (în continuare-Aplicația). Aplicația este destinată atât exprimării e-votului de către alegător, cât și verificării e-votului exprimat de către el. Aplicația trebuie să dispună de o componentă de backend în scop de interoperabilitate cu Sistemul de Management e-Votare și cu sisteme/servicii externe.

### 7.2.1 CU 02.01 Identificarea și autentificarea alegătorului în Aplicația Alegătorului

Cazul de utilizare este destinat autentificării alegătorului  în aplicația alegătorului.
Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.2.1.1** | Obligatorie | Aplicația trebuie să permită integrarea cu mecanismele guvernamentale de autentificare a alegătorilor (MPass și altele). |
| **7.2.1.2** | Obligatorie | După autentificarea reușită, Aplicația trebuie să poată să identifice și să valideze alegătorul. |
| **7.2.1.3** | Obligatorie | Aplicația trebuie să poată să recepționeze date personale din Lista electorală aferente alegătorului (cel puțin următoarele date: IDNP, Nume, Prenume, Sexul, Data nașterii, Date adresă, Secția de Votare). |
| **7.2.1.4** | Obligatorie | Aplicația trebuie să stocheze datele personale ale alegătorului cu afișarea lor ulterioară pe parcursul procedurii de votare prin internet. |

| | | |
|---|---|---|
| **7.2.1.5** | Obligatorie | Aplicația trebuie să permită invalidarea alegătorilor înainte de și în procesul votării (de ex., dacă mecanismul de autentificare a votantului a fost compromis, acesta trebuie blocat). |
| **7.2.1.6** | Obligatorie | În scop de criptare a e-votului ce urmează a fi exprimat pentru fiecare scrutin disponibil alegătorului aplicația va obține cheia publică din Sistemul de Management E-votare. |
| **7.2.1.7** | Obligatorie | Pentru fiecare scrutin, aplicația trebuie să recepționeze certificatul electronic al cheii publice în scop de semnare digitală a datelor e-votului ce urmează a fi exprimat. |
| **7.2.1.8** | Obligatorie | În caz că Aplicația este realizată ca o aplicație mobilă, atunci după autentificarea MPass reușită trebuie să fie blocate sesiunile de autentificare de pe alte dispozitive mobile. |
| **7.2.1.9** | Obligatorie | Luând în considerație de perioada de timp în care nu este posibil votarea repetată, aplicația va prezenta alegătorului una din opțiuni: votare sau verificare a votului. |
| **7.2.1.10** | Obligatorie | În caz că Aplicația este realizată ca o aplicație mobilă, atunci după autentificarea MPass reușită aplicația mobilă trebuie sa dispună de autentificarea locală cu amprenta digitală sau Face ID. |

### 7.2.2 CU 02.02. Prezentarea buletinelor de vot electronice în Aplicația Alegătorului

Cazul de utilizare este destinat afișării datelor buletinelor de vot electronice în Aplicația Alegătorului. Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.2.2.1** | Obligatorie | După identificare și autentificarea Alegător, Aplicația trebuie să dispună de mecanism de descărcare automată de date aferente buletinelor electronice de vot relevante alegătorului:<br>- lista de scrutine<br>- circumscripții electorale pentru fiecare scrutin lista de opțiuni de votare pentru fiecare scrutin și circumscripție electorală<br>- hash-ul datelor scrutinului (datele incluse in hash vor fi decise pe parcursul implementării)<br>- metadate relevante buletinelor de vot, cum ar fi antet, culoare, font, sigla concurentului electoral, ordinea afișării opțiunilor de votare și alte date. |
| **7.2.2.2** | Obligatorie | Aplicația trebuie să stocheze datele aferent buletinelor electronice de vot cu afișarea lor ulterioară pe parcursul procedurii de votare electronică. |
| **7.2.2.3** | Obligatorie | Aplicația trebuie să permită alegătorului să vizualizeze toate scrutinele separat și pentru fiecare scrutin buletinul de vot electronic cu toate opțiunile de votare. |
| **7.2.2.4** | Obligatorie | Aplicația trebuie să permită selectarea unei singure opțiuni de votare din fiecare buletin de vot pentru fiecare scrutin. |

| | | |
|---|---|---|
| **7.2.2.5** | Obligatorie | Opțiunile de votare trebuie să apară într-un format clar, inteligibil, conform metadatelor setate și fără a fi codificate. |

### 7.2.3 CU 02.03. Selectarea și confirmarea opțiunilor de votare în Aplicația Alegătorului

Cazul de utilizare este destinat selectării și confirmarea opțiunilor de votare în Aplicația Alegătorului.
Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.2.3.1** | Obligatorie | Aplicația trebuie să valideze toate acțiunile utilizatorului pentru a preveni erorile pe parcursul procesului de vot. |
| **7.2.3.2** | Obligatorie | Aplicația trebuie să permită selectarea de opțiuni numai din lista opțiunilor descărcate. |
| **7.2.3.3** | Obligatorie | Aplicația trebuie să afișeze clar deosebirea dintre opțiunea selectată de cele neselectate. |
| **7.2.3.4** | Obligatorie | Aplicația trebuie să permită alegătorului să verifice opțiunile de votare înainte de a confirma votul. |
| **7.2.3.5** | Obligatorie | Aplicația trebuie să asigure alegătorul cu mecanism de modificare a opțiunii de votare selectate înainte de a o confirma (pentru fiecare buletin de vot electronic pentru fiecare scrutin și circumscripție). |
| **7.2.3.6** | Obligatorie | Aplicația trebuie să asigure alegătorul cu mecanism de confirmare a votului selectat. |

### 7.2.4 CU 02.04. Exprimare e-votului în Aplicația Alegătorului

Cazul de utilizare este destinat procesului de exprimare a e-votului de către alegător pentru fiecare buletin de vot electronic prin intermediul Aplicației Alegătorului.
Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.2.4.1** | Obligatorie | Aplicația trebuie asigure secretul votului pin criptare datele aferent votului confirmat (scrutinul, circumscripția electorală, lista opțiunilor de votare, votul exprimat și un număr aleatoriu necesar procedurii de verificare a votului exprimat) pentru fiecare buletin de vot electronic. |
| **7.2.4.2** | Obligatorie | Aplicația trebuie să folosească un algoritm de criptare asimetric, astfel încât e-voturile criptate cu cheia publică să nu poată fi decriptate cu aceeași cheie. Voturile trebuie să fie decriptate doar cu cheia privată. |
| **7.2.4.3** | Obligatorie | Aplicarea algoritmului asimetric de criptare trebuie să permită<br>a. generarea unui număr de criptotexte egal cu numărul de opțiuni din lista opțiunilor pentru fiecare scrutin și fiecare circumscripție electorală. |

| | | |
|---|---|---|
| | | b. toate criptotextele să fie criptări ale valorii 0, cu excepția criptotextului care va corespunde opțiunii pentru care alegătorul își exprimă votul. Acest criptotext este o criptare a valorii 1.<br>c. fiecare criptotext trebuie să fie completat cu o dovadă criptografică care demonstrează că criptotextul este o criptare a unei valori booleene (0 sau 1). Acest lucru nu permite alegătorul să-și exprime mai mult de o opțiune.<br>d. criptotextele trebuie să fie completate cu o dovadă, care demonstrează că suma valorilor opțiunilor din lista de opțiuni este 1. Și acest lucru nu-i va permite alegătorului să selecteze mai mult de o opțiune din listă.<br>e. trebuie să utilizeze la criptare un număr aleator, care<br>i. va face ca aceiași opțiune exprimată să genereze criptotexte diferite<br>ii. se va folosi de către Alegător pentru verificarea e-votului exprimat de el și fără a cunoaște cheia decriptării (doar cu cunoașterea acestui număr aleator și al codului tranzacției). |
| **7.2.4.4** | Obligatorie | După criptarea e-votului confirmat, Aplicația trebuie să solicite Alegătorului aplicarea semnăturii digitale peste date e-votant și date aferent e-voturilor confirmate (identificatorul scrutinul, identificatorul unic al circumscripției electorale, listei opțiunilor de vot, criptotextele (ordonate conform opțiunile din buletinele de vot) și dovezile. |
| **7.2.4.5** | Obligatorie | După aplicarea semnăturii digitale peste datele e-votant și date e-vot confirmat trebuie să fie transmise în Sistemul de Management e-Votare.<br>e-Votul criptat (setul de criptotexte) transmis în Sistemul de Management e-Votare va fi considerat ca **e-vot exprimat**. |
| **7.2.4.6** | Obligatorie | Aplicația trebuie să fie capabilă să recepționeze de la Sistemul de Management e-Votare și să afișeze confirmarea recepționării e-votului exprimat. |
| **7.2.4.7** | Obligatorie | Aplicația trebuie să fie capabilă să recepționeze de la Sistemul de Management e-Votare și să afișeze un cod pentru verificarea e-votului exprimat. |
| **7.2.4.8** | Obligatorie | Aplicația trebuie să permită exprimarea e-votul doar în intervalul de timp destinat e-votării (parametri setați în sistem). În caz contrar, aplicația trebuie să informeze alegătorul despre imposibilitatea exprimării e-votului. |
| **7.2.4.9** | Obligatorie | Aplicația trebuie să permită alegătorului să voteze repetat după o perioadă de timp predefinită (parametru setat în sistem). |

Notă: Un exemplu de realizare a acestor tehnici este descris în următoarea lucrare https://eprint.iacr.org/2016/776.

### 7.2.5 CU 02.05. Verificarea e-votului exprimat în Aplicația Alegătorului

Cazul de utilizare este destinat verificării votului exprimat de către alegător prin intermediul în aplicației Alegătorului.
Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.2.5.1** | Obligatorie | Aplicația trebuie să asigure alegătorul cu o funcționalitate care să-i permită să verifice dacă e-votul exprimat de el este înregistrat în Sistemul de Management e-Votare. |
| **7.2.5.2** | Obligatorie | Aplicația trebuie să asigure alegătorul cu o funcționalitate care să-i permită să verifice dacă opțiunea selectată de alegător este acea opțiune care este stocată în sistem. |
| **7.2.5.3** | Obligatorie | Verificarea trebuie fie făcută pe bază de un cod/un număr unic recepționat în Aplicația Alegătorului e-Votare din Sistemul de Management e-Votare după confirmarea e-votul exprimat. |
| **7.2.5.4** | Obligatorie | Aplicația trebuie să permită alegătorului să verifice votul numai într-o perioadă de timp predefinită (parametru setat în sistem) după confirmarea recepționării e-votului exprimat. |
| **7.2.5.5** | Obligatorie | Aplicația trebuie să permită verificarea votului exprimat inclusiv de pe un alt dispozitiv după autentificarea prealabilă a alegătorului. |

## 7.3 Cazuri de utilizare din Componenta ”Colector”

În acest compartiment sunt prezentate cerințele funcționale pentru cazurile de utilizare din Componenta ”Colector” a Sistemului Management e-Votare. Componenta este destinată

- Înregistrării și stocării de date e-votanți și e-voturi exprimate
- de transmitere date e-votare către Componenta ”Procesator”.

### 7.3.1 CU 03.01. Înregistrare e-voturi exprimate

Cazul de utilizare este destinat înregistrării în Sistemul de Management e-Votare a e-voturilor exprimate în componenta Colector și în Blockchain.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.3.1.1** | Obligatorie | Sistemul trebuie să dispună de Serviciu de recepție tranzacții din aplicația alegătorului e-Votare aferent e-votantului și a e-voturilor exprimate pentru fiecare scrutin și circumscripție electorală. |
| **7.3.1.2** | Obligatorie | Sistemul trebuie să poată să verifice datele recepționate din Aplicația Alegătorului: |

| | | |
|---|---|---|
| | | a. autenticitatea și integritatea Aplicației Alegătorului.<br>b. corectitudinea semnăturii digitale aplicată peste tranzacție<br>c. corectitudinea dovezilor criptografice din interiorul tranzacției privind e-votul exprimat, adică dacă alegătorul a exprimat o singură opțiune (fără a putea identifica opțiunea exprimată). |
| **7.3.1.3** | Obligatorie | Sistemul trebuie să poată stoca în BD datele recepționate din aplicația alegătorului e-Votare. |
| **7.3.1.4** | Obligatorie | Sistemul trebuie să poată aplica și stoca marcaj de timp peste tranzacțiile recepționate. |
| **7.3.1.5** | Obligatorie | Sistemul trebuie să poată calcula și stoca<br>- hash-ul tranzacției (arbore Merkle)<br>- hash-ul blocului de tranzacții (arbore Merkle). |
| **7.3.1.6** | Obligatorie | Sistemul trebuie să asigure că e-voturile exprimate nu pot fi modificate (falsificate) în timpul păstrării acestora. |
| **7.3.1.7** | Obligatorie | Colectorul trebuie să asigure că e-voturile exprimate nu pot fi șterse/radiate/distruse/înlăturate în timpul păstrării acestora. |
| **7.3.1.8** | Obligatorie | În scop de asigurare imposibilitate modificare și distrugere e-voturi exprimate, sistemul trebuie să asigure ca hash-urile e-voturilor exprimate să fie stocate într-o rețea Blockchain privată. |
| **7.3.1.9** | Obligatorie | Sistemul trebuie să permită înregistrarea și stocarea de date e-votanți și e-voturi exprimate doar în intervalul de timp destinat e-votării (parametri setați de administrator). |

### 7.3.2 CU 03.02. Export date e-votare din Colector

Cazul de utilizare este destinat gestionării proceselor de export date e-votare din cadrul componentei Colector.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.3.2.1** | Obligatorie | Sistemul trebuie să dispună de **interfață** care asigură gestionarea proceselor de export date e-votare din cadrul componentei Colector. |
| **7.3.2.2** | Obligatorie | Sistemul trebuie să dispună de serviciu de export e-voturi exprimate și e-votanți pe dispozitiv de stocare date (în scop de transmitere date în componenta Procesator). |
| **7.3.2.3** | Obligatorie | Sistemul trebuie să dispună de serviciu de export e-votanți pe dispozitiv de stocare date (în scop de transmitere date în SI ”Ziua votului” (EDay)). |
| **7.3.2.4** | Obligatorie | Structura datelor destinate exportului se va determina la etapa de dezvoltare a sistemului. |
| **7.3.2.5** | Obligatorie | Serviciile de import din cadrul componentei sunt accesate de către Organizator. |

| | | |
|---|---|---|
| **7.3.2.6** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de operațiuni de import/export din cadrul componentei. |
| **7.3.2.7** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de import/export date. |

### 7.3.3 CU 03.03. Interoperabilitate cu Aplicația Alegătorului

Cazul de utilizare este destinat interoperabilității Sistemului Management e-Votare cu Aplicația Alegătorului e-votare.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.3.3.1** | Obligatorie | Sistemul trebuie să dispună de un serviciu dedicat de interoperabilitate cu aplicațiile alegătorului. |
| **7.3.3.2** | Obligatorie | Sistemul trebuie să aibă capacitatea de a transmite în aplicația alegătorului e-Votare date personale alegător (cel puțin următoarele date: IDNP, Nume, Prenume, Sexul, Data nașterii, Date adresă, Secția de Votare). |
| **7.3.3.3** | Obligatorie | Sistemul trebuie să aibă capacitatea de a transmite în aplicația alegătorului e-Votare date despre scrutine din ziua alegerilor, circumscripția electorală la care este asignat alegătorul pentru scrutinele din ziua alegerilor, date opțiuni de votare. |
| **7.3.3.4** | Obligatorie | Sistemul trebuie să aibă capacitatea de a transmite în aplicația alegătorului e-Votare metadate privind buletinele de vot (sigla partid, ordinea amplasării opțiunii în buletin, ...). |
| **7.3.3.5** | Obligatorie | Sistemul trebuie să aibă capacitatea de a transmite informație relevantă în aplicația alegătorului e-Votare (spre exemplu, mesaje în caz neidentificare or nevalidare alegător, adrese de verificare e-votul exprimat, codul de verificare a e-votului exprimat, cheia publică de criptare e-vot, date algoritm de criptare e-vot, alte informații relevante). |
| **7.3.3.6** | Obligatorie | Sistemul trebuie să dispună de serviciu de transmitere în Aplicația Alegătorului confirmare de înregistrare e-vot exprimat și numărul unic al tranzacției atribuit în colector. În caz de nevalidare date sistemul va expedia mesaje aferente. |
| **7.3.3.7** | Obligatorie | Sistemul trebuie să dispună de serviciu de recepție solicitare a alegătorului de verificare date e-vot exprimat în baza numărului unic al tranzacției din colector. |
| **7.3.3.8** | Obligatorie | Sistemul trebuie să dispună de serviciu de transmitere în Aplicația Alegătorului date privind verificarea e-votului exprima în baza numărului unic al tranzacției<br>o prezenței votului în Sistemul de Management e-Votare<br>o corectitudinea stocării e-votului exprimat (opțiunea exprimată în e-votul stocat în Sistem este opțiunea exprimată de către Alegător). |

### 7.3.4 CU 03.04. Interoperabilitate cu sisteme externe

Cazul de utilizare este destinat interoperabilității Sistemului Management e-Votare cu sisteme externe.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.3.4.1** | Obligatorie | Sistemul trebuie să dispună de serviciu dedicat pentru transmitere a hash-urilor aferent e-votului exprimat în rețele Blockchain. |
| **7.3.4.2** | Obligatorie | Sistemul trebuie să transmită hash-urile aferent e-votului exprimat și a blocurilor de e-voturi exprimate în structura blockchain privat. |
| **7.3.4.3** | Obligatorie | Sistemul trebuie să semneze blocuri cu semnătură digitală. |

## 7.4 Cazuri de utilizare din Componenta ”Procesator”

Componenta este destinată procesării e-voturilor exprimate și trebuie să dispună de servicii de procesare a datelor pentru fiecare din pașii:

- Verificarea integrității e-voturilor exprimate
- Anularea e-voturilor recurente
- Anularea e-voturilor dublate (care sunt exprimate și la secția de votare)
- Anonimizarea e-voturilor

De asemenea, componenta trebuie să mai dispună de servicii de import/export date e-votare și de instrumente de gestiune serviciile de procesare, cum ar fi lansare/oprire/relansare/ștergere date.

### 7.4.1 CU 04.01. Import/export date e-votare în/din Procesator

Cazul de utilizare este destinat gestionării proceselor de import/export din cadrul componentei Procesator a Sistemului de Management e-Votare.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.4.1.1** | Obligatorie | Sistemul trebuie să dispună de **interfață** care asigură gestionarea proceselor de import/export din cadrul componentei Procesator. |
| **7.4.1.2** | Obligatorie | Sistemul trebuie să dispună de serviciu de import listă e-votanți și e-voturi exprimate de pe dispozitiv extern de stocare de date (date exportate din Colector). |
| **7.4.1.3** | Obligatorie | Sistemul trebuie sa asigure un mecanism de verificare a integrității datelor importate. |
| **7.4.1.4** | Obligatorie | Sistemul trebuie să dispună de serviciu de import **listă votanți la secțiile de votare** de pe dispozitiv extern de stocare de date (date exportate din SI ”Ziua votului” (EDay)). |

| | | |
|---|---|---|
| **7.4.1.5** | Obligatorie | Sistemul trebuie să dispună de serviciu de export e-voturi pe dispozitiv extern de stocare de date (destinate numărării e-voturilor exprimate). |
| **7.4.1.6** | Obligatorie | Structura datelor destinate importului/exportului se va determina la etapa de dezvoltare a sistemului. |
| **7.4.1.7** | Obligatorie | Serviciile de import/export din cadrul componentei sunt accesate de către Organizator. |
| **7.4.1.8** | Obligatorie | Sistemul trebuie să dispună de structură de stocare date importate. |
| **7.4.1.9** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de operațiuni de import/export din cadrul componentei. |
| **7.4.1.10** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de import/export date. |

### 7.4.2 CU 04.02. Utilizare instrumente pentru servicii de procesare date e-votare

Cazul de utilizare este destinat descrierii instrumentelor necesare serviciilor de procesare date e-votare din Componenta Procesator a Sistemului de Management e-Votare.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.4.2.1** | Obligatorie | Sistemul trebuie să dispună de **interfață** destinată utilizării instrumentelor pentru serviciile de procesare date e-votare: lansare/oprire/relansare/ștergere date. |
| **7.4.2.2** | Obligatorie | Instrumentele din cadrul componentei sunt accesate de către Organizator. |
| **7.4.2.3** | Obligatorie | Procesarea e-voturilor exprimate trebuie să se realizeze într-un mediu off-line izolat. |
| **7.4.2.4** | Obligatorie | Procesarea e-voturilor trebuie să aibă loc după încheierea perioadei de vot și înainte de numărarea voturilor. |
| **7.4.2.5** | Obligatorie | Procesatorul trebuie să jurnalizeze evenimentele legate de accesarea serviciilor din cadrul componentei. |
| **7.4.2.6** | Obligatorie | Procesatorul trebuie să ducă evidența statistică a indicatorilor legați de procesarea e-voturilor exprimate. |
| **7.4.2.7** | Obligatorie | Instrumentele sunt utilizate numai după finalizarea procesării datelor de la fiecare pas. |
| **7.4.2.8** | Obligatorie | Consecutivitatea pașilor procesării e-voturilor exprimate este următoarea:<br>• Verificarea integrității e-voturilor exprimate<br>• Anularea e-voturilor recurente<br>• Anularea e-voturilor dublate<br>• Anonimizarea e-voturilor<br>• |

### 7.4.3 CU 04.03. Verificarea integrității e-voturilor exprimate

Cazul de utilizare este destinat descrierii cerințelor față de serviciul de la pasul de verificare a integrității e-voturilor exprimate.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.4.3.1** | Obligatorie | Sistemul trebuie să dispună de **serviciu de verificare** a integrității e-voturilor exprimate. |
| **7.4.3.2** | Obligatorie | Sistemul trebuie să verifice integritatea structurii e-voturilor importate (prezența tuturor proprietăților, marcajelor, dovezilor, alte verificări de integritate). |
| **7.4.3.3** | Obligatorie | Verificarea integrității trebuie să fie făcută separat pentru fiecare scrutin și fiecare circumscripție electorală. |
| **7.4.3.4** | Obligatorie | E-voturile exprimate trebuie să fie grupate pe scrutine și pe circumscripții. |
| **7.4.3.5** | Obligatorie | Sistemul trebuie să poată să emită un proces verbal privind lista voturilor neintegre, să le mute într-un registru separat și care nu vor fi procesate ulterior. |
| **7.4.3.6** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de verificarea integrității e-voturilor exprimate. |
| **7.4.3.7** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de verificarea integrității e-voturilor exprimate. |

### 7.4.4 CU 04.04. Anularea e-voturilor recurente

Cazul de utilizare este destinat descrierii cerințelor față de serviciul de la pasul de anulare a e-voturilor recurente.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.4.4.1** | Obligatorie | Sistemul trebuie să dispună de **serviciu de anulare a e-voturilor recurente**. Va rămâne doar ultimul e-vot exprimat de către alegător. |
| **7.4.4.2** | Obligatorie | Anularea trebuie să fie făcută separat pentru fiecare scrutin și fiecare circumscripție electorală. |
| **7.4.4.3** | Obligatorie | E-voturile exprimate trebuie să fie grupate pe scrutine și pe circumscripții. |
| **7.4.4.4** | Obligatorie | Identificarea e-voturilor recurente trebuie să fie făcută pe bază de IDNP. |
| **7.4.4.5** | Obligatorie | Sistemul trebuie să țină cont că același alegător poate să-și exprime e-votul multiplu. |
| **7.4.4.6** | Obligatorie | Pentru procesarea ulterioară a e-voturilor trebuie să rămână doar ultimul e-vot exprimat conform marcajului de timp aplicat. |

| | | |
|---|---|---|
| **7.4.4.7** | Obligatorie | Sistemul trebuie să poată să emită un proces verbal privind lista voturilor recurente, să le mute într-un registru separat și care nu vor fi procesate ulterior. |
| **7.4.4.8** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de anularea e-voturilor recurente. |
| **7.4.4.9** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de anularea e-voturilor exprimate recurente. |

### 7.4.5 CU 04.05. Anularea e-voturilor dublate

Cazul de utilizare este destinat descrierii cerințelor față de serviciul de la pasul de anulare a voturilor dublate exprimate și în secția de votare (e-vot dublat).

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.4.5.1** | Obligatorie | Sistemul trebuie să dispună de **serviciu de anulare a e-voturilor dublate**. |
| **7.4.5.2** | Obligatorie | E-votul exprimat de alegător este considerat dublat dacă este exprimat de către alegător și la secția de votare cu prezența fizică. |
| **7.4.5.3** | Obligatorie | Exprimarea votului cu prezența fizică la secția de votare va anula votul exprimat prin internet. |
| **7.4.5.4** | Obligatorie | Pasul trebuie să poate fi lansat numai dacă sunt importate datele din SI Ziua Votului. |
| **7.4.5.5** | Obligatorie | Identificarea e-voturilor dublate trebuie să fie făcută pe bază de IDNP. |
| **7.4.5.6** | Obligatorie | Anularea trebuie să fie făcută separat pentru fiecare scrutin și fiecare circumscripție electorală. |
| **7.4.5.7** | Obligatorie | E-voturile exprimate trebuie să fie grupate pe scrutine și pe circumscripții. |
| **7.4.5.8** | Obligatorie | Sistemul trebuie să poată să emită un proces verbal privind lista voturilor dublate, să le mute într-un registru separat și care nu vor fi procesate ulterior. |
| **7.4.5.9** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de anularea e-voturilor exprimate în secția de votare. |
| **7.4.5.10** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de anularea e-voturilor exprimate în secția de votare. |

### 7.4.6 CU 04.06. Anonimizare e-voturi exprimate

Cazul de utilizare este destinat descrierii cerințelor față de serviciul de la pasul de anonimizare a e-voturilor exprimate.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|

| | | |
|---|---|---|
| **7.4.6.1** | Obligatorie | Sistemul trebuie să dispună de **serviciu de anonimizare** a e-voturilor exprimate prin separarea datelor personale ale e-votantului de e-votul exprimat. |
| **7.4.6.2** | Obligatorie | Sistemul trebuie să șteargă și alte date care ar putea face legătura dintre e-votant și e-vot exprimat, cum ar fi marcaj de timp, hash-uri calculate și alte date. |
| **7.4.6.3** | Obligatorie | Anonimizarea trebuie să fie făcută separat pentru fiecare scrutin și fiecare circumscripție electorală. |
| **7.4.6.4** | Obligatorie | E-voturile exprimate trebuie să fie grupate pe scrutine și pe circumscripții. |
| **7.4.6.5** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de anularea e-voturilor exprimate în secția de votare. |
| **7.4.7.6** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de anularea e-voturilor exprimate în secția de votare. |

## 7.5 Cazuri de utilizare din Componenta ”Contor”

Componenta este destinată numărării e-voturilor exprimate și trebuie să dispună de instrumente care să asigurare executarea etapelor.

Etapele de numărare a e-voturilor exprimate sunt următoarele:

- Activarea cheii private pentru inițiere numărare
- Numărarea voturilor criptate
- Distrugerea cheii private și a artefactelor

### 7.5.1 CU 05.01. Import/export date e-votare în/din Contor

Cazul de utilizare este destinat gestionării proceselor de import/export din cadrul componentei Contor a Sistemului de Management e-Votare.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.5.1.1** | Obligatorie | Sistemul trebuie să dispună de **interfață** care asigură gestionarea proceselor de import/export din cadrul componentei Contor. |
| **7.5.1.2** | Obligatorie | Sistemul trebuie să dispună de serviciu de import listă e-voturi anonimizate de pe dispozitiv extern de stocare de date (date exportate din Colector). |
| **7.5.1.3** | Obligatorie | Sistemul trebuie să dispună de serviciu de export rezultat numărare e-voturi anonimizate pe dispozitiv extern de stocare de date (destinate decriptării și deanonimizării opțiunilor în modulul HSM ). |
| **7.5.1.4** | Obligatorie | Structura datelor destinate importului/exportului se va determina la etapa de dezvoltare a sistemului. |

| | | |
|---|---|---|
| **7.5.1.5** | Obligatorie | Serviciile de import/export din cadrul componentei sunt accesate de către Organizator. |
| **7.5.1.6** | Obligatorie | Sistemul trebuie să dispună de structură de stocare date importate. |
| **7.5.1.7** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de operațiuni de import/export din cadrul componentei. |
| **7.5.1.8** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de import/export date. |

### 7.5.2 CU 05.02. Utilizare instrumente pentru serviciu de numărare e-voturi

Cazul de utilizare este destinat descrierii instrumentelor pe care trebuie le serviciul de numărare e-voturi din Componenta Contor a Sistemului de Management e-Votare.

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.5.2.1** | Obligatorie | Sistemul trebuie să dispună de **interfață** destinată utilizării instrumentelor pentru serviciul de numărare e-voturi anonimizate și criptate: lansare/oprire/relansare/ștergere date. |
| **7.5.2.2** | Obligatorie | Instrumentele din cadrul componentei sunt utilizate de către Organizator. |
| **7.5.2.3** | Obligatorie | Numărarea e-voturilor exprimate trebuie să se realizeze într-un mediu off-line izolat. |
| **7.5.2.4** | Obligatorie | Numărarea e-voturilor trebuie să aibă loc după procesarea e-voturilor. |

### 7.5.3 CU 05.03. Numărarea voturilor criptate

Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.5.3.1** | Obligatorie | Sistemul trebuie să dispună de **serviciu de numărare** e-voturi anonimizate și criptate. |
| **7.5.3.2** | Obligatorie | Sistemul trebuie să verifice integritatea structurii e-voturilor importate. |
| **7.5.3.3** | Obligatorie | Verificarea integrității trebuie să fie făcută separat pentru fiecare scrutin și fiecare circumscripție electorală. |
| **7.5.3.4** | Obligatorie | Pentru numărare e-voturile anonimizate și criptate trebuie să fie grupate pe scrutine, pe circumscripții și pe fiecare opțiune de votare. |
| **7.5.3.5** | Obligatorie | Numărarea e-voturilor criptate și anonimizate pe scrutine, pe circumscripții și pe fiecare opțiune de votare trebuie să fie făcută cu utilizarea proprietății aditiv homomorfice a algoritmului de criptare. |

| | | |
|---|---|---|
| **7.5.3.6** | Obligatorie | În rezultatul numărării sistemul va crea tranzacții totalizatorii cu rezultat de numărare e-voturi criptate pentru fiecare scrutin, circumscripție și opțiune de votare (fără a putea identifica opțiunea). |
| **7.5.3.7** | Obligatorie | Numărarea e-voturilor trebuie să fie făcută separat pentru fiecare scrutin și fiecare circumscripție electorală. |
| **7.5.3.8** | Obligatorie | Sistemul trebuie să fie capabil să sumeze e-voturile exprimate pe opțiuni, scrutine și pe circumscripții electorale. |
| **7.5.3.9** | Obligatorie | Sistemul trebuie să fie capabil să emită o dovadă de numărare cu zero cunoștințe (a zero-knowledge-proof), care poate fi utilizată pentru a dovedi corectitudinea numărării e-voturilor. |
| **7.5.3.10** | Obligatorie | Sistemul trebuie să fie capabil să emită un proces verbal cu rezultat numărare e-voturi anonimizate și criptate. |
| **7.5.3.11** | Obligatorie | Procesul verbal trebuie să fie semnat digital de Membrii CEE. |
| **7.5.3.12** | Obligatorie | Sistemul trebuie să jurnalizeze evenimentele legate de numărarea e-voturilor exprimate. |
| **7.5.3.13** | Obligatorie | Sistemul trebuie să ducă evidența statistică a indicatorilor legați de numărarea e-voturilor exprimate. |

## 7.6 CU 06. Observare proces e-votare

Cazul de utilizare este destinat observării procesului e-Votare de către observator extern prin intermediul Sistemului de Observare e-Votare.
Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.6.1** | Obligatorie | Observatorul extern trebuie să dispună de o interfață dedicată observării procesului de e-votare utilizând instrumente software open-source pre aprobate. |
| **7.6.2** | Obligatorie | Observatorul extern trebuie să poată:<br>- să verifice integritatea tranzacțiilor<br>- să verifice dovezile criptografice ale e-voturilor<br>- să verifice corectitudinea cantității de tranzacții în Colector și Blockchain-uri<br>- să verifice corectitudinea tranzacției totalizatorii cu rezultat numărare e-voturi criptate<br>- să verifice dovezile criptografice ale corectitudinii decriptării rezultatului numărării e-voturilor. |
| **7.6.3** | Obligatorie | Sistemul de observare e-votare trebuie să se asigure de faptul că instrumentele de monitorizare nu pot compromite confidențialitatea votantului și acuratețea alegerilor. |
| **7.6.4** | Obligatorie | Sistemul de e-votare trebuie să asigure instrumente de monitorizare care să poată detecta orice anomalie în procesul de vot. |
| **7.6.5** | Obligatorie | Sistemul de e-votare trebuie să asigure faptul că instrumentele de monitorizare sunt rezistente la falsificare și asigură nerespingerea informațiilor de audit înregistrate. |

| | | |
|---|---|---|
| **7.6.6** | Obligatorie | Sistemul de e-votare trebuie să asigure instrumente de monitorizare care să permită detectarea oricărei modificări în cadrul sistemului certificat și al componentelor aplicațiilor instalate pe platforma de vot. |
| **7.6.7** | Recomandare | Se recomandă ca sistemul de e-votare să poată asigura instrumente de monitorizare bazate pe jurnalizări de sistem și de aplicații, fără a necesita acces la componentele platformei de vot. |
| **7.6.8** | Recomandare | Se recomandă ca sistemul de e-votare să poată asigura instrumente de monitorizare, dotate cu un sistem de alertare, care analizează jurnalizările de sistem și de aplicație pe baza riscurilor de securitate și permite analizarea și investigarea incidentelor posibile. |

## 7.7 CU 07. Afișare KPI

Cazul de utilizare este destinat afișării KPI.
Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.7.1** | Obligatorie | Instrumentele de monitorizare ale sistemului de e-votare trebuie să includă informație analitică despre mersul e-votării. Această informație trebuie să poate fi descărcată pe dispozitive de stocare date. |
| **7.7.2** | Obligatorie | Informația analitică despre mersul e-votării trebuie să cuprindă cel puțin următoarele categorii de date privind alegători:<br><br>- număr total de alegători autentificați în aplicația alegătorului<br>- număr total de alegători autorizați în aplicația alegătorului<br>- număr total de alegători cu buletine electronice de vot recepționate per fiecare scrutin<br>- numărul total de alegători cu buletine electronice de vot expediate per fiecare scrutin. |
| **7.7.3** | Obligatorie | Informația analitică despre mersul e-votării trebuie să cuprindă cel puțin următoarele categorii de date privind buletinele electronice de vot cu vot exprimat per fiecare scrutin și circumscripție electorală:<br><br>- număr total de e-voturi exprimate<br>- număr total de e-voturi exprimate stocate în colector<br>- număr total de e-voturi exprimate exportate pentru a fi transmise la procesare<br>- număr total de e-voturi exprimate importate pentru a fi procesate<br>- număr total de e-voturi exprimate procesate<br>- număr total de e-voturi exprimate procesate anulate din motiv de vot recurență<br>- număr total de e-voturi exprimate procesate anulate din motiv de dublare<br>- număr total de e-voturi exprimate procesate valabile |

| | | |
|---|---|---|
| | | - număr total de e-voturi exprimate procesate exportate pentru a fi transmise la numărare<br>- număr total de e-voturi exprimate importate pentru a fi numărate<br>- număr total de e-voturi exprimate numărate pe fiecare scrutin, circumscripție, opțiune de votare.<br>- număr total de e-voturi exprimate numărate pe fiecare scrutin, circumscripție, opțiune de votare exportate pentru a fi decriptate în modulul HSM. |
| **7.7.4** | Obligatorie | Informația analitică trebuie să fie afișată în Internet. Actualizare informațiilor trebuie să fie făcută la fiecare interval de timp presetat (intervalul se va stabili la etapa de elaborare a Sistemului). |
| **7.7.5** | Obligatorie | Accesul la indicatorii statistici trebuie să fie disponibil tuturor utilizatorilor cu rolurile de Organizator și Membru CEE. |

## 7.8 CU 08. Jurnalizare evenimente

Cazul de utilizare este destinat acțiunilor de administrare utilizate în cadrul SI e-Votare.
Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.8.1** | Obligatorie | Sistemul de e-votare trebuie să dispună de instrumente de jurnalizare a tuturor evenimentelor de la etapele și pașii procesului de e-votare din sistem. |
| **7.8.2** | Obligatorie | Sistemul de e-votare trebuie să dispună de instrumente de descărcare jurnale a evenimentelor. |

## 7.9 CU 09. Autentificare

Cazul de utilizare este destinat autentificării utilizatorilor în Sistemul de Management e-Votare și în Sistemul Observare e-Votare.
Cerințele funcționale aferent cazului de utilizare sunt prezentate în tabelul de mai jos.

| ID | Importanță | Cerință |
|---|---|---|
| **7.9.1** | Obligatorie | Sistemul de Management e-Votare trebuie să permită integrarea cu mecanismele guvernamentale de autentificare a alegătorilor (MPass și altele). |
| **7.9.2** | Obligatorie | În rezultatul autentificării reușite, utilizatorii cu rolurile de Organizator și Membru CEE vor dispune de acces la Sistemul de Management e-Votare în conformitate cu accesul descris în cazurile de utilizare. |
| **7.9.3** | Obligatorie | Sistemul de Observare e-Votare trebuie să permită integrarea cu mecanismele guvernamentale de autentificare a alegătorilor (MPass și altele). |

| | | |
|---|---|---|
| **7.9.4** | Obligatorie | În rezultatul autentificării reușite, utilizatorii cu rolurile de Observator vor dispune de acces la Sistemul de Observare e-Votare în conformitate cu accesul descris în cazurile de utilizare. |

# 8 Cerințele non-funcționale

## 8.1 Cerințe de securitate

### 8.1.1 Securitatea cap la cap

| ID | Importanță | Cerință |
|---|---|---|
| CnF.1. | Obligatorie | Sistemul trebuie să securizeze prin criptare e-voturile exprimate pe aplicația alegătorului înainte de fi transmise în Sistemul de Management e-Votare. |
| CnF.2. | Obligatorie | Sistemul trebuie să asigure că numai Comisia Electorală Centrală poate decripta rezultatul numărării e-voturilor exprimate. |
| CnF.3. | Obligatorie | Sistemul trebuie să fie verificabil cap la cap, să conțină dovezi criptografice care asigură, în afara oricăror dubii, corectitudinea operațiunilor executate de componentele Sistemul de Management e-Votare (adică, trebuie să asigure verificabilitatea dacă votul a fost exprimat cum s-a intenționat și a fost numărat așa cum a fost exprimat). |
| CnF.4. | Obligatorie | Aplicația Alegătorului trebuie să comunice Sistemul de Management e-Votare utilizând protocolul HTTPS și trebuie să valideze certificatul backend-ului (TLS pinning). |
| CnF.5. | Obligatorie | Cheia publică generată pentru fiecare scrutin trebuie să fi semnată cu un certificat. |
| CnF.6. | Obligatorie | La recepționarea informațiilor despre scrutine aplicația alegătorului trebuie să valideze semnătura cheii publice cu certificatul. |

### 8.1.2 Confidențialitatea alegătorilor

| ID | Importanță | Cerință |
|---|---|---|
| CnF.7. | Obligatorie | Sistemul trebuie să asigure că voturile sunt criptate astfel încât doar Comisia Electorală Centrală să le poată decripta. |
| CnF.8. | Obligatorie | Sistemul trebuie să asigure că, cheia necesară pentru decriptarea voturilor nu este disponibilă (adică nu există) în procesul de vot până când Comisia Electorală Centrală o recuperează/reconstruiește. |
| CnF.9. | Obligatorie | Sistemul trebuie să asigure că cel puțin o majoritate predefinită a membrilor Comisiei Electorale Centrale este necesară în vederea recuperării cheii de decriptare. |
| CnF.10. | Obligatorie | Sistemul trebuie să asigure că nu este posibil de corelat ordinea în care voturile au fost decriptate cu ordinea în care acestea au fost exprimate. |
| CnF.11. | Obligatorie | Sistemul trebuie să asigure faptul că două voturi diferite cu același conținut au forma de criptare diferită. |
| CnF.12. | Obligatorie | Orice proces de control susținut de sistem pentru verificarea acurateței alegerilor nu trebuie să compromită confidențialitatea votantului. |
| CnF.13. | Obligatorie | Sistemul trebuie să asigure că voturile sunt criptate astfel încât doar Comisia Electorală Centrală să le poată decripta. |

### 8.1.3 Eligibilitatea votanților

| ID | Importanță | Cerință |
|---|---|---|
| CnF.14. | Obligatorie | Sistemul trebuie să asigure că numai alegătorii eligibili au acces la platforma de vot. |
| CnF.15. | Obligatorie | Înainte de acceptarea unui vot exprimat, sistemul trebuie să verifice identitatea alegătorului care a exprimat votul. |
| CnF.16. | Obligatorie | Sistemul trebuie să permită verificarea, la orice oră în timpul alegerilor, că voturile electronice din urna electorală aparțin alegătorilor (recepționarea confirmării digitale a votului pe Internet și un acces securizat de autentificare prin intermediul SIVI). |
| CnF.17. | Obligatorie | Sistemul trebuie să asigure nerepudierea voturilor exprimate. |
| CnF.18. | Obligatorie | Sistemul nu trebuie să aibă informații despre rechizitele alegătorilor necesare pentru protecția nerepudierii votului. |
| CnF.19. | Obligatorie | Sistemul trebuie să prevină includerea în urna electorală a unor buletine fictive de către utilizatorii externi și administratorii de sistem. |
| CnF.20. | Obligatorie | Sistemul trebuie să utilizeze certificate electronice unice pentru autentificarea alegătorilor. |
| CnF.21. | Obligatorie | Sistemul trebuie să utilizeze certificatul electronic unic al votantului pentru semnarea digitală a voturilor exprimate. |
| CnF.22. | Obligatorie | |

### 8.1.4 Confidențialitatea votului

| ID | Importanță | Cerință |
|---|---|---|
| CnF.23. | Obligatorie | Sistemul trebuie să asigure că votul exprimat este secret în raport cu orice terț, inclusiv administratori de sistem și potențiali hackeri care sparg măsurile convenționale de securitate de protecție a platformei de vot. |
| CnF.24. | Obligatorie | Voturile trebuie să fie criptate pe terminalul votantului înainte de a fi exprimate. |
| CnF.25. | Obligatorie | Voturile pot fi decriptate numai de Comisia Electorală Centrală. |
| CnF.26. | Obligatorie | Sistemul trebuie să prevină decriptarea voturilor înainte de încheierea alegerilor pentru a evita scurgerea de informații privind rezultatele parțiale. |
| CnF.27. | Obligatorie | Orice proces de control susținut de sistem pentru a verifica acuratețea alegerilor nu trebuie să compromită secretul votului. |

### 8.1.5 Integritatea votului

| ID | Importanță | Cerință |
|---|---|---|
| CnF.28. | Obligatorie | Sistemul trebuie să păstreze în procesul electoral integritatea fiecărui vot individual exprimat. |
| CnF.29. | Obligatorie | Sistemul trebuie să permită verificarea integrității fiecărui vot individual stocat în urna electorală. |
| CnF.30. | Obligatorie | Integritatea votului este protejată de alegător când își exprimă votul. |
| CnF.31. | Obligatorie | Sistemul trebuie să prevină orice tentativă de a include buletine fictive în urna electorală digitală. |

| | | |
|---|---|---|
| CnF.32. | Obligatorie | Alegătorii folosesc certificatele electronice proprii pentru a-și proteja voturile prin semnătura digitală. |

### 8.1.6 Precizia/acuratețea urnei electorale

| ID | Importanță | Cerință |
|---|---|---|
| CnF.33. | Obligatorie | Sistemul trebuie să permită verificarea integrității și identității serviciului care gestionează urna electorală, înainte de a lansa procesul de decriptare și contabilizare a voturilor. |
| CnF.34. | Obligatorie | Sistemul trebuie să prevină orice tentativă de a include buletine fictive de către utilizatorii externi și administratorii de sistem. |
| CnF.35. | Obligatorie | Sistemul, în scopuri de control, trebuie să permită urmărirea exactă a proceselor care s-au încheiat cu exprimarea și stocarea votului într-o urnă electorală. |
| CnF.36. | Obligatorie | Sistemul trebuie să aplice măsuri adecvate pentru detectarea oricărei tentative de a șterge un vot din urna electorală. |
| CnF.37. | Obligatorie | Sistemul poate avea componente segregate în diferite servicii, astfel încât fiecare serviciu să poată verifica funcționarea corectă a celorlalte servicii în vederea garantării integrității urnei electorale și a altor date electorale. |
| CnF.38. | Obligatorie | Sistemul trebuie să publice conținutul informațiilor din urna electorală în timpul și după procesul de vot pentru a permite alegătorilor să verifice prezența voturilor lor în urna electorală, într-o manieră anonimă. |

### 8.1.7 Comisia Electorală Centrală

| ID | Importanță | Cerință |
|---|---|---|
| CnF.39. | Obligatorie | Sistemul utilizează o schemă/prag/plafon alcătuit/ă din N membri din numărul total M pentru membrii Comisiei Electorale Centrale în scopul recuperării cheii care permite decriptarea voturilor. |
| CnF.40. | Obligatorie | Niciun membru individual al CEC sau un grup de membri sub pragul stabilit nu trebuie să aibă posibilitatea de a recupera cheia care permite decriptarea voturilor. |
| CnF.41. | Obligatorie | Sistemul trebuie să susțină utilizarea unor dispozitive inviolabile (de ex., cartele inteligente protejate prin PIN) pentru stocarea informațiilor necesare de către fiecare membru al Comisiei Electorale Centrale în vederea recuperării ulterioare a cheii pentru decriptarea voturilor. |
| CnF.42. | Obligatorie | Schema pragului este bazată pe schema de partajare a secretului sau pe o schemă similară. |
| CnF.43. | Obligatorie | Cheia de decriptare nu există până când nu este reconstruită de membrii CEC la încheierea alegerilor. |

### 8.1.8 Verificabilitatea votantului

| ID | Importanță | Cerință |
|---|---|---|
| CnF.44. | Obligatorie | Sistemul trebuie să permită alegătorilor să verifice dacă votul lor a fost prezent în procesul de decriptare și contabilizare, pe baza recipisei de votare. |
| CnF.45. | Obligatorie | Sistemul trebuie să permită alegătorilor să verifice dacă voturile lor sunt prezente în urna electorală după ce au fost exprimate.Procesul de verificare a recipisei de votare trebuie să permită detectarea recipiselor manipulate sau fictive pentru a preveni plângeri frauduloase din partea alegătorilor. |
| CnF.46. | Obligatorie | Sistemul trebuie să permită alegătorilor să verifice dacă votul lor a for stocat adecvat în sistem (de ex., prin coduri de răspuns).Sistemul trebuie să permită alegătorilor să verifice dacă voturile lor sunt prezente în urna electorală după ce au fost exprimate. |
| CnF.47. | Obligatorie | Sistemul trebuie să asigure aplicarea metodei de verificare a votului exprimat independent de softul clientului votant (de ex., folosind canalele alternative). Sistemul trebuie să permită alegătorilor să verifice dacă votul lor a for stocat adecvat în sistem (de ex., prin coduri de răspuns). |
| CnF.48. | Obligatorie | Sistemul trebuie să asigure aplicarea metodei de verificare a votului exprimat independent de softul clientului votant (de ex., folosind canalele alternative). |
| CnF.49. | Obligatorie | |

### 8.1.9 Prevenirea impunerii și comercializării votului

| ID | Importanță | Cerință |
|---|---|---|
| CnF.50. | Obligatorie | Sistemul trebuie să genereze dovezi criptografice de verificare (de ex., recipisa de votare) care să nu le permită alegătorilor să demonstreze unui terț pentru cine au votat. |
| CnF.51. | Obligatorie | Sistemul trebuie să prevină orice tentativă a unei persoane de a corela voturile cu alegătorii. |
| CnF.52. | Obligatorie | Procesele care rup corelarea voturilor cu alegătorii ar trebui să fie universal verificabile, generând dovezi criptografice care nu manipulează rezultatele, fără a compromite cheile criptografice private folosite în proces (de ex., cu ajutorul Zero Knowledge Proofs). |
| CnF.53. | Obligatorie | Dovezile criptografice generate de sistem, care permit alegătorilor să verifice dacă voturile lor au fost stocate adecvat în sistem, nu trebuie să faciliteze niciodată practici de impunere a votantului sau practici de comercializare a voturilor. Pot fi puse în aplicare măsuri suplimentare, cum ar fi voturile multiple, în vederea prevenirii acestui fenomen. |

### 8.1.10 Auditabilitatea independentă

| ID | Importanță | Cerință |
|---|---|---|
| CnF.54. | Obligatorie | Sistemul trebuie să permită urmărirea în sens invers a procesului alegerilor, într-o manieră semnificativă, fără a compromite confidențialitatea sau acuratețea alegerilor. |
| CnF.55. | Obligatorie | Informațiile jurnalizate de sistem și informațiile despre alegeri generate în timpul alegerilor trebuie să permită efectuarea unui control adecvat al alegerilor. |
| CnF.56. | Obligatorie | Sistemul trebuie să pună în aplicare practici criptografice adecvate pentru verificarea acurateței și integrității informațiilor jurnalizate care urmează să fie utilizate în timpul controlului. |
| CnF.57. | Obligatorie | Sistemul trebuie să permită oricărui observator independent să verifice și să certifice integritatea componentelor aplicației în orice moment în timpul alegerilor. |
| CnF.58. | Obligatorie | Se recomandă ca sistemul de vot să asigure instrumente de monitorizare care să poată detecta orice modificare operată sistemului certificat și componentelor aplicației instalate pe platforma de vot. |
| CnF.59. | Obligatorie | Se recomandă ca sistemul de vot să asigure instrumente de monitorizare bazate pe jurnalele de sistem și de aplicații, fără a fi nevoie de acces la componentele platformei de vot. |
| CnF.60. | Obligatorie | Se recomandă ca sistemul de vot să asigure un sistem de alertare, folosind jurnalul de sistem și cel de aplicație, bazate pe analiza securității, care să permită analizarea și investigarea incidentelor posibile. |
| CnF.61. | Obligatorie | Se recomandă ca sistemul de vot să asigure instrumente de monitorizare care permit verificarea integrității componentelor sistemului în raport cu amprentele de bază. |
| CnF.62. | Obligatorie | Procesul de decriptare și contabilizare trebuie să asigure dovezi criptografice precum că voturile nu au fost manipulate în cadrul acestor procese. Dovezile criptografice ar trebui să fie verificabile de orice terț autorizat, fără a compromite informațiile sensibile, care permit efectuarea corelării dintre voturile decriptate și alegători. |

### 8.1.11 Disponibilitatea serviciului

| ID | Importanță | Cerință |
|---|---|---|
| CnF.63. | Obligatorie | Sistemul trebuie să fie scalabil fără ca să sisteze serviciul. |
| CnF.64. | Obligatorie | Sistemul trebuie să fie tolerant la erori. |
| CnF.65. | Obligatorie | Sistemul trebuie să pună în aplicare practici care atenuează atacurile de tipul blocarea accesului. |

## 8.2 Posibilitatea de utilizare și accesibilitatea

### 8.2.1 Posibilitatea de utilizare

| ID | Importanță | Cerință |
|---|---|---|

| | | |
|---|---|---|
| CnF.66. | Obligatorie | Sistemul ar trebui să-i asigure alegătorului o interfață ușor de utilizat, astfel încât procesul de vot să fie la nivel intuitiv, fără a necesita instruire pentru folosirea canalului de votare. |
| CnF.67. | Obligatorie | Alegătorul nu ar trebui să fie impus să instaleze vreun certificat electronic specific pe dispozitivul de exprimare a votului. |
| CnF.68. | Obligatorie | Sistemul trebuie să susțină utilizarea motoarelor de căutare principale și a sistemelor operaționale. |
| CnF.69. | Obligatorie | Sistemul trebuie să includă instrucțiuni inteligibile pentru alegători. |
| CnF.70. | Obligatorie | Sistemul trebuie să avertizeze alegătorii în cazul în care, în procesul de votare, ei au selectat o opțiune care ar putea să le invalideze votul (de ex., au selectat mai puține opțiuni decât este necesar/undervoting, au selectat mai multe opțiuni decât este necesar/overvoting, …). |
| CnF.71. | Obligatorie | Alegătorii trebuie să aleagă opțiunile de votare, selectând direct candidatul, în loc să folosească un cod sau o metodă de selectare indirectă. |

### 8.2.2 Accesibilitatea

| ID | Importanță | Cerință |
|---|---|---|
| CnF.72. | Obligatorie | Sistemul trebuie să susțină utilizarea mai multor limbi fără să compromită confidențialitatea votantului. |
| CnF.73. | Obligatorie | Sistemul trebuie să fie conform cu standardele de accesibilitate WGAI70. |

## 8.3 Scalabilitatea și flexibilitatea

| ID | Importanță | Cerință |
|---|---|---|
| CnF.74. | Obligatorie | Sistemul trebuie să permită completarea cu noi componente, fără a sista serviciul. |
| CnF.75. | Obligatorie | Sistemul ar trebui să aibă capacitatea de a organiza alegeri pentru mii și milioane de alegători într-o manieră facilă și cost-eficientă. |
| CnF.76. | Obligatorie | Sistemul trebuie să susțină toate caracteristicile procesului electoral corespunzător al țării. |
| CnF.77. | Obligatorie | Sistemul trebuie să fie adaptabil în ceea ce privește mai multe particularități, cum ar fi aspectul, limba, ajutor și paginile cu informații etc. care să fie conforme cerințelor autorității electorale. |
| CnF.78. | Obligatorie | Sistemul trebuie să susțină câteva mecanisme pentru autentificarea alegătorilor. Aceste mecanisme ar trebui să aibă capacitatea de a funcționa în paralel, astfel încât să poată fi maximizată rata de participare. |
| CnF.79. | Obligatorie | Instrumentele de gestionare ale sistemului trebuie să fie adaptabile cerințelor autorității electorale, cum ar fi capacitatea de a accesa rata de participare în timp real, de a inspecta sistemul sau de a anula/revoca anumite voturi, urmând procedurile agreate. |

## 8.4 Conformitatea cu standardele

| ID | Importanță | Cerință |
|---|---|---|
| CnF.80. | Obligatorie | Sistemul trebuie să susțină cerințele Codului electoral al RM și reglementările asociate. |
| CnF.81. | Obligatorie | Sistemul trebuie să fie compatibil/conform cu standardele electorale ale Consiliului Europei. |
| CnF.82. | Obligatorie | Sistemul trebuie să fie compatibil/conform cu Election Markup Language (EML) – https://en.wikipedia.org/wiki/Election_Markup_Language. |
| CnF.83. | Obligatorie | Orice algoritm criptografic utilizat în sistem trebuie să fie bazat pe standarde deschise. |

## 8.5 Codul-sursă al soft-ului/produsului program

| ID | Importanță | Cerință |
|---|---|---|
| CnF.84. | Obligatorie | Codul sursă al aplicației și sistemelor platformei de votare prin internet trebuie să fie publicat în scop ca publicul larg pentru a fi analizat și auditat. |

## 8.6 Activități de administrare

| ID | Importanță | Cerință |
|---|---|---|
| CnF.85. | Obligatorie | Sistemul de vot trebuie să se asigure de faptul că instrumentele de monitorizare nu pot compromite confidențialitatea votantului și acuratețea alegerilor. |
| CnF.86. | Obligatorie | Sistemul de vot trebuie să asigure instrumente de monitorizare care să poată detecta orice anomalie în procesul de vot. |
| CnF.87. | Obligatorie | Sistemul trebuie să asigure faptul că instrumentele de monitorizare sunt rezistente la falsificare și asigură nerespingerea informațiilor de audit înregistrate. |
| CnF.88. | Obligatorie | Sistemul de vot ar trebui să asigure instrumente de monitorizare care să permită detectarea oricărei modificări în cadrul sistemului certificat și al componentelor aplicațiilor instalate pe platforma de vot. |
| CnF.89. | Obligatorie | Se recomandă ca sistemul de vot să poată asigura instrumente de monitorizare bazate pe jurnalizări de sistem și de aplicații, fără a necesita acces la componentele platformei de vot. |
| CnF.90. | Obligatorie | Se recomandă ca sistemul de vot să poată asigura instrumente de monitorizare, dotate cu un sistem de alertare, care analizează jurnalizările de sistem și de aplicație pe baza riscurilor de securitate și permite analizarea și investigarea incidentelor posibile. |

## 8.7 Cerințe modul HSM

| ID | Importanță | Cerință |
|---|---|---|
| CnF.91. | Obligatorie | Modulul HSM trebuie să fie compatibil cu standardul PKCS 11. |
| CnF.92. | Obligatorie | Modulul HSM trebuie să dispună de generarea a unei chei și distribuirea a accesului la aceasta la mai multe persoane. |
| CnF.93. | | |
| CnF.94. | Obligatorie | Modulul HSM trebuie să poată genera perechi de chei (publică și privată) pentru fiecare scrutin din ziua alegerilor. |
| CnF.95. | Obligatorie | Cheile publice (pentru fiecare scrutin din ziua alegerilor) sunt plasate pe servere și, ulterior, transmise în Aplicațiile Alegătorului. |
| CnF.96. | | |
| CnF.97. | Obligatorie | Modulul HSM trebuie să mențină algoritm de criptare homomorfică (de ex. algoritmul ELGamal or altul). |
| CnF.98. | Obligatorie | Modulul HSM nu trebuie să permite descărcarea cheii private. |
| CnF.99. | Obligatorie | Modulul HSM trebuie să poată demonstra că decriptarea datelor (tranzacțiilor) încărcate în modulul HSM privind rezultatul numărării e-voturilor criptate a avut loc corect. |
| CnF.100. | Obligatorie | Modulul HSM trebuie să dispună de instrument de distrugere de chei private după o perioadă de timp. |
| CnF.101. | Obligatorie | Decriptarea e-voturilor numărate poate fi făcută numai cu cheia privată de decriptare generată în pereche cu cheia publică de criptare e-voturi exprimate. |
| CnF.102. | Obligatorie | Perechea de chei publică de criptare și privată de decriptare e-voturi exprimate este generată până la declanșarea procesului de e-votare. |
| CnF.103. | Obligatorie | Decriptarea e-voturilor numărate poate fi început numai după identificarea (inserarea) numărului prestabilit de părți de cheie privată de decriptare deținute de membrii CEE. |
| CnF.104. | Obligatorie | Părțile de cheie privată a membrilor CEE trebuie să fie sigilate pentru prevenirea multiplicării și fraudării cheilor. |