

Ministerul Finanţelor

CAIET DE SARCINI

Realizarea sistemului informatic integrat şi centralizat al trezoreriei statului (eTrezor)

Cuprins

[1. Informaţii generale 1](#_Toc125958906)

[1.1. Autoritatea contractantă 1](#_Toc125958907)

[1.2. Beneficiarul proiectului 1](#_Toc125958908)

[1.3. Grup ţintă 1](#_Toc125958909)

[1.4. Data de începere şi perioada de execuţie a contractului 1](#_Toc125958910)

[1.5. Localizare 1](#_Toc125958911)

[1.6. Proiecte desfăşurate sau în curs de desfăşurare care pot avea impact asupra contractului 1](#_Toc125958912)

[2. Scopul și obiectivele proiectului 2](#_Toc125958913)

[2.1. Scopul proiectului 2](#_Toc125958914)

[2.2. Obiectivele specifice ale proiectului 2](#_Toc125958915)

[3. Supoziții și riscuri 2](#_Toc125958916)

[3.1. Supoziții care fundamentează implementarea proiectului 2](#_Toc125958917)

[3.2. Riscuri principale 2](#_Toc125958918)

[4. Prezentarea contextului și actorilor de business 3](#_Toc125958919)

[4.1. Serviciul Decontări și Relații cu Sistemul Interbancar de Plăți din cadrul Direcției Generale de Contabilitate Publică 4](#_Toc125958920)

[4.2. Trezoreria Operativă Centrală din cadrul Direcției Generale de Contabilitate Publică 5](#_Toc125958921)

[4.3. Activitatea de Trezorerie și Contabilitate Publică din cadrul Direcției Generale Regionale a Finanțelor Publice / Administrației Județene a Finanțelor Publice 5](#_Toc125958922)

[4.4. Activitatea de Trezorerie și Contabilitate Publică a Municipiului București, Trezoreriile Sectoarelor Municipiului București, din cadrul Direcției Generale Regionale a Finanțelor Publice București 6](#_Toc125958923)

[4.5. Unități teritoriale ale trezoreriei statului din cadrul Activităților de Trezorerie și Contabilitate Publică din cadrul Direcțiilor Generale Regionale ale Finanțelor Publice / Administrațiilor Județene ale Finanțelor Publice 6](#_Toc125958924)

[5. Descrierea sistemelor informatice existente 6](#_Toc125958925)

[5.1. Aplicația TREZOR 6](#_Toc125958926)

[5.1.1. Funcționalități asigurate de aplicația TREZOR 6](#_Toc125958927)

[5.1.2. Rapoarte generate din TREZOR 10](#_Toc125958928)

[5.1.3. Arhivarea datelor din TREZOR 11](#_Toc125958929)

[5.1.4. Tehnologia TREZOR 11](#_Toc125958930)

[5.2. Aplicația TAXEDIV 11](#_Toc125958931)

[5.2.1. Funcționalități asigurate de aplicația TAXEDIV 12](#_Toc125958932)

[5.2.2. Interconectarea aplicației 12](#_Toc125958933)

[5.2.3. Sisteme necesare aplicației 12](#_Toc125958934)

[5.3. Aplicația de administrare de depozite (DEPTERM) 13](#_Toc125958935)

[5.3.1. Funcționalități asigurate de aplicația DEPTERM 13](#_Toc125958936)

[5.4. Aplicația de administrare de certificate de trezorerie (EMICERT-EMIRAP) 13](#_Toc125958937)

[5.4.1. Aplicația EMICERT 13](#_Toc125958938)

[5.4.2. Aplicația EMIRAP 14](#_Toc125958939)

[5.5. Aplicația CASHBNR 15](#_Toc125958940)

[5.5.1. Funcționalități asigurate de aplicația CASHBNR 15](#_Toc125958941)

[5.5.2. Interconectarea aplicației CASHBNR 15](#_Toc125958942)

[5.5.3. Sisteme necesare aplicației CASHBNR 15](#_Toc125958943)

[5.6. Aplicația Cont Tranzitoriu 16](#_Toc125958944)

[5.6.1. Funcționalități asigurate de Cont Tranzitoriu 16](#_Toc125958945)

[5.6.2. Interconectarea aplicației Cont Tranzitoriu 16](#_Toc125958946)

[5.6.3. Sisteme necesare aplicației Cont Tranzitoriu 17](#_Toc125958947)

[5.7. Aplicația de deschideri de credite Dcredite 17](#_Toc125958948)

[5.7.1. Funcționalități asigurate de aplicația Dcredite 17](#_Toc125958949)

[5.7.2. Interconectarea aplicației Dcredite 18](#_Toc125958950)

[5.7.3. Sisteme necesare aplicației 18](#_Toc125958951)

[5.8. Aplicația de deschideri de credite pentru bugetul trezoreriei statului Dcredite\_BTS 19](#_Toc125958952)

[5.8.1. Funcționalități asigurate de aplicația Dcredite\_BTS 19](#_Toc125958953)

[5.9. Aplicația Ibancls10g 19](#_Toc125958954)

[5.9.1. Funcționalități asigurate de aplicația Ibancls10g 19](#_Toc125958955)

[5.9.2. Interconectarea aplicației Ibancls10g 19](#_Toc125958956)

[5.10. Alte aplicații informatice 19](#_Toc125958957)

[5.11. Aplicația de înrolare a utilizatorilor instituții publice și administratori din trezorerie (Înrolare Forexebug) 20](#_Toc125958958)

[5.12. Sistemul FOREXEBUG 20](#_Toc125958959)

[5.12.1. Punctul Unic de Acces – Portal ForExeBug 21](#_Toc125958960)

[5.12.2. Sistemul National de Mesagerie (ForexeSNM) 21](#_Toc125958961)

[5.12.3. DEDOC - Platforma electronica de depunere documente 22](#_Toc125958962)

[5.12.4. Nomenclatoare generale (ForexeNOMEN) 22](#_Toc125958963)

[5.12.5. Aplicatia Control Angajamente Bugetare (CAB) 22](#_Toc125958964)

[5.12.6. Raportare bugete 23](#_Toc125958965)

[5.12.7. Raportare situații financiare 23](#_Toc125958966)

[5.12.8. Raportare execuție bugetară 23](#_Toc125958967)

[5.12.9. Depozitul central de date (ForExeBug DW) 23](#_Toc125958968)

[5.12.10. Generarea rapoartelor standard și ad-hoc de către sistemul național de raportare ForExeBug 23](#_Toc125958969)

[5.13. Spațiul Privat Virtual 24](#_Toc125958970)

[5.14. Descrierea infrastructurii de retea a MF/ANAF 24](#_Toc125958971)

[5.15. Descrierea sistemului de balansare aplicații cu F5 Networks 25](#_Toc125958972)

[5.16. Descrierea serviciului de management al identității și control acces TIM/TAM 27](#_Toc125958973)

[5.17. Descrierea situației actuale la nivelul Beneficiarului 30](#_Toc125958974)

[5.17.1. Servere pentru SGBD 31](#_Toc125958975)

[5.17.2. Infrastructura de comunicații InfiniBand 32](#_Toc125958976)

[5.17.3. Infrastructura de stocare 32](#_Toc125958977)

[5.17.4. Infrastructura rețelei SAN 33](#_Toc125958978)

[5.17.5. Infrastructura de comunicații Ethernet 33](#_Toc125958979)

[5.17.6. Soluția de administrare platforme informatice 33](#_Toc125958980)

[5.17.7. Baze de date 34](#_Toc125958981)

[5.17.8. Soluția hardware-software pentru efectuarea și restaurarea salvărilor de siguranță 34](#_Toc125958982)

[5.18. Descriere mecanisme de integrare 35](#_Toc125958983)

[5.18.1. Forexebug 35](#_Toc125958984)

[5.18.2. SIAC 37](#_Toc125958985)

[5.18.3. NOES 38](#_Toc125958986)

[5.18.4. SAIVEN 38](#_Toc125958987)

[5.18.5. FTY-Star 38](#_Toc125958988)

[5.18.6. QpayIntegrator 38](#_Toc125958989)

[5.18.7. E-popriri 38](#_Toc125958990)

[6. Cerințe generale ale soluției eTrezor 39](#_Toc125958991)

[6.1. Cerințe funcționale ale soluției 40](#_Toc125958992)

[6.2. Cerințe aplicabile platformei on-line 45](#_Toc125958993)

[6.3. Cerințe privind modulul de raportare și analiză 45](#_Toc125958994)

[6.4. Cerințe modul de management al documentelor 46](#_Toc125958995)

[6.5. Cerințe soluție de înrolare a utilizatorilor 48](#_Toc125958996)

[6.6. Asigurarea continuității funcționării sistemului eTrezor 51](#_Toc125958997)

[7. Cerințe funcționale specifice 51](#_Toc125958998)

[7.1. Cerințe funcționale specifice core banking 51](#_Toc125958999)

[7.2. Cerinte functionale specifice Internet banking 52](#_Toc125959000)

[7.3. Cerințe functionale specifice solutiei de prezentare (portal) 54](#_Toc125959001)

[8. Cerințe instruire 55](#_Toc125959002)

[9. Schimbarea cerințelor 55](#_Toc125959003)

[10. Cerințe tehnice ale soluției eTrezor 55](#_Toc125959004)

[10.1. Cerințe generale 55](#_Toc125959005)

[10.1.1. Accesibilitate (Accessibility) 60](#_Toc125959006)

[10.1.2. Administrare (Service Management) 60](#_Toc125959007)

[10.1.3. Audit și Control (Audit and Control) 60](#_Toc125959008)

[10.1.4. Baze de date (Databases) 61](#_Toc125959009)

[10.1.5. Backup 63](#_Toc125959010)

[10.1.6. Colectare date (Data Entry) 63](#_Toc125959011)

[10.1.7. Disponibilitate (Availability) 64](#_Toc125959012)

[10.1.8. Documentație (Documentation) 65](#_Toc125959013)

[10.1.9. Fluxuri de lucru (Workflows) 65](#_Toc125959014)

[10.1.10. Integrare (Integration) 66](#_Toc125959015)

[10.1.11. Monitorizare (Monitoring) 66](#_Toc125959016)

[10.1.12. Performanță (Performance) 67](#_Toc125959017)

[10.1.13. Platforma (Platform) 68](#_Toc125959018)

[10.1.14. Programare rulare job-uri (Job Scheduling) 68](#_Toc125959019)

[10.1.15. Securitate (Security) 69](#_Toc125959020)

[10.2. Cerințe non-funcționale core banking 70](#_Toc125959021)

[10.2.1. Capacitate (Capacity) 70](#_Toc125959022)

[10.2.2. Colectare date (Data Entry) 71](#_Toc125959023)

[10.2.3. Dezvoltare (Development) 71](#_Toc125959024)

[10.2.4. Metadate (Metadata) 71](#_Toc125959025)

[10.2.5. Raportare (Reporting) 72](#_Toc125959026)

[10.2.6. Raportare Operațională (Operational Reporting) 74](#_Toc125959027)

[10.2.7. Securitate 75](#_Toc125959028)

[10.2.8. Utilizabilitate (Usability) 75](#_Toc125959029)

[10.3. Cerințe non-funcționale Internet Banking 76](#_Toc125959030)

[10.4. Cerințe non-funcționale portal 77](#_Toc125959031)

[10.5. Cerințe non-funcționale soluție de înrolare a utilizatorilor 78](#_Toc125959032)

[10.6. Cerințe componenta de integrare fluxuri 79](#_Toc125959033)

[10.7. Cerințe platforma de document management (DMS) 81](#_Toc125959034)

[10.8. Cerințe soluție de disaster recovery 83](#_Toc125959035)

[10.9. Estimări de capacitate şi planificare 84](#_Toc125959036)

[10.10. Scalabilitate, disponibilitate ridicată, performanţă 84](#_Toc125959037)

[10.11. Cerințe server web 85](#_Toc125959038)

[10.12. Cerințe server de aplicații 86](#_Toc125959039)

[10.13. Platforma de securizare a accesului la resurse 87](#_Toc125959040)

[10.13.1. Soluția de control al accesului și administrare a conturilor de utilizator de portal trebuie să îndeplinească următoarele condiții (minime și obligatorii): 88](#_Toc125959041)

[10.13.2. Stocarea profilelor de utilizatori în cadrul soluției trebuie să se realizeze folosind o soluție care respectă următoarele cerințe: 90](#_Toc125959042)

[10.14. Platforma de integrare la nivel de date 91](#_Toc125959043)

[10.15. Soluție de securizare a comunicațiilor 92](#_Toc125959044)

[10.15.1. Echipament router 92](#_Toc125959045)

[10.15.2. Echipament switch 95](#_Toc125959046)

[10.15.3. Echipamente dedicate pentru securizare perimetrală (2 bucăți, în configurație redundantă) 97](#_Toc125959047)

[10.15.4. Echipament dedicat pentru management, logare și raportare 98](#_Toc125959048)

[10.16. Soluție hardware-software pentru efectuarea și restaurarea salvărilor de siguranță 100](#_Toc125959049)

[10.16.1. Platformă pentru efectuarea și restaurarea salvărilor de siguranță 100](#_Toc125959050)

[10.16.2. Echipament pentru efectuarea salvărilor de siguranță pe disc 104](#_Toc125959051)

[10.16.3. Biblioteci de benzi 105](#_Toc125959052)

[10.16.4. Benzi de date LTO 8 RW 106](#_Toc125959053)

[10.16.5. Benzi de date LTO-8 WORM 107](#_Toc125959054)

[10.16.6. Rack-uri pentru instalarea componentelor hardware 107](#_Toc125959055)

[10.17. Soluție audit, monitorizare și securitate 107](#_Toc125959056)

[11. Descrierea activităților proiectului 109](#_Toc125959057)

[11.1. Analiza și proiectarea sistemului eTrezor 109](#_Toc125959058)

[11.1.1. Rezultate 110](#_Toc125959059)

[11.1.2. Documente generate 110](#_Toc125959060)

[11.2. Construirea soluției pentru sistemul eTrezor 111](#_Toc125959061)

[11.2.1. Rezultate 111](#_Toc125959062)

[11.2.2. Documente generate 111](#_Toc125959063)

[11.3. Pregătirea mediului de testare 113](#_Toc125959064)

[11.3.1. Planificarea testelor 113](#_Toc125959065)

[11.3.2. Dezvoltarea şi execuţia testelor 113](#_Toc125959066)

[11.3.3. Coordonarea testelor 113](#_Toc125959067)

[11.3.4. Managementul testării şi raportării 113](#_Toc125959068)

[11.3.5. Livrabile din testare 114](#_Toc125959069)

[11.3.6. Rezultate 115](#_Toc125959070)

[11.3.7. Documente generate 115](#_Toc125959071)

[11.4. Instalarea și configurarea infrastructurii hardware și software (licențe software de bază) a sistemului 115](#_Toc125959072)

[11.4.1. Rezultate 115](#_Toc125959073)

[11.4.2. Documente generate 115](#_Toc125959074)

[11.5. Instalarea și configurarea sistemului eTrezor, pe mediul de producție, migrarea datelor și punerea sistemului în funcțiune. 115](#_Toc125959075)

[11.5.1. Rezultate 116](#_Toc125959076)

[11.5.2. Documente generate 116](#_Toc125959077)

[11.6. Asistarea Beneficiarului în realizarea testelor de acceptanță. 116](#_Toc125959078)

[11.6.1. Criterii de acceptanţă 116](#_Toc125959079)

[11.6.2. Procedura de acceptanţă 116](#_Toc125959080)

[11.6.3. Rezultate 117](#_Toc125959081)

[11.6.4. Documente generate 117](#_Toc125959082)

[11.7. Mentenanță corectivă și adaptivă a sistemului după acceptarea acestuia. 117](#_Toc125959083)

[11.7.1. Rezultate 118](#_Toc125959084)

[11.7.2. Documente generate 118](#_Toc125959085)

[11.8. Instruire 118](#_Toc125959086)

[11.8.1. Realizare curriculă 118](#_Toc125959087)

[11.8.2. Realizarea materialelor de instruire pentru formatori și utilizatori 119](#_Toc125959088)

[11.8.3. Instruirea formatorilor Beneficiarului (train the trainers) 119](#_Toc125959089)

[11.8.4. Instruirea utilizatorilor speciali (administratori de aplicație) 120](#_Toc125959090)

[11.8.5. Furnizarea de cursuri pentru personalul de specialitate TIC (dezvoltatori, administratori de sistem) 120](#_Toc125959091)

[12. Garanția sistemului 121](#_Toc125959092)

[13. Glosar de termeni și abrevieri utilizate 122](#_Toc125959093)

# Informaţii generale

Realizarea sistemului informatic integrat şi centralizat al trezoreriei statului (eTrezor).

## Autoritatea contractantă

Autoritatea Contractantă este Ministerul Finanțelor.

## Beneficiarul proiectului

Beneficiarul proiectului este Ministerul Finanțelor.

## Grup ţintă

Grupul ţintă al proiectului este compus din angajați din cadrul aparatului central al Ministerului Finanțelor și angajați din cadrul unităților teritoriale ale trezoreriei statului (factori de decizie și personal operațional).

## Data de începere şi perioada de execuţie a contractului

Data de începere a contractului este prima zi lucrătoare după îndeplinirea cumulativă a următoarelor condiţii:

1. semnarea contractului de către ambele părți
2. constituirea de către Consultant a garanției de bună execuție.

Oferta Consultantului va fi realizată ţinând cont de termenul de finalizare a contractului din PNRR, 31.12.2025.

## Localizare

Activităţile proiectului vor fi realizate în România, la sediul Ministerului Finantelor, Centrului National pentru Informatii Financiare, Centrului Secundar de Date din Brasov sau în cadrul unităților subordonate, în locațiile indicate de Beneficiar.

Locaţia principală pentru desfășurarea operaţiunilor aferente Proiectului va fi Municipiul Bucureşti, unde Consultantul trebuie să dispună de resursele materiale, umane, financiare și informaționale necesare derulării activităţilor. În cadrul proiectului, Consultantul va suporta toate costurile generate de deplasările la sediile Beneficiarului sau în cadrul unităților subordonate.

## Proiecte desfăşurate sau în curs de desfăşurare care pot avea impact asupra contractului

1. în cadrul ANAF se află în implementare proiectul „Servicii fiscale eficiente pentru administrație și cetățeni - SFERA", prin intermediul căruia se dorește modernizarea sistemelor informatice utilizate de MF pentru gestionarea declarațiilor fiscale depuse de contribuabili și urmărirea conformării la declarare și plată a acestora, pentru evidența și gestionarea eficientă a creanțelor fiscale și bugetare cuvenite bugetului general consolidat, pentru rambursarea eficientă a taxei pe valoarea adăugată și a accizelor și pentru gestionarea executărilor silite.
2. SIPOCA737 – arhiva electronică

# Scopul și obiectivele proiectului

## Scopul proiectului

Ministerul Finanțelor, prin prezentul caiet de sarcini, îşi propune consolidarea capacităţii administrației publice prin dezvoltarea și implementarea unui sistem centralizat și integrat de efectuare a operaţiunilor de încasări şi plăţi, prin Trezoreria Statului și oferirea de servicii de tip internet banking pentru clienții Trezoreriei Statului.

## Obiectivele specifice ale proiectului

1. Centralizarea sistemului informatic al trezoreriei statului și îmbunătățirea / optimizarea perioadelor de decontare a instrumentelor de plată utilizate în relație cu Trezoreria Statului;
2. Diversificarea modalităților de realizare a operațiunilor de plăți efectuate de către clienții cu conturi deschise la unitățile trezoreriei statului prin dezvoltarea unei platforme de tip internet banking;
3. Obținerea de informaţii agregate şi în timp real cu privire la operaţiunile de încasări şi plăţi;
4. Instruirea angajaţilor de la nivelul aparatului central al Ministerului Finanţelor şi din cadrul unităţilor teritoriale ale trezoreriei statului în utilizarea sistemelor informatice dezvoltate în cadrul proiectului.

# Supoziții și riscuri

## Supoziții care fundamentează implementarea proiectului

1. Atitudinea proactivă a tuturor structurilor implicate, cu privire la participarea reprezentanţilor la activităţi dedicate realizării proiectului.
2. Existența unor abilităţi şi cunoştinţe adecvate pentru personalul MF / ANAF / DGRFP în ceea ce privește procesele derulate prin intermediul unităților trezoreriei statului.

## Riscuri principale

1. Nu toate cerințele sunt evaluate în timpul fazei de analiză
2. Lipsa de comunicare internă şi externă cu privire la proiect şi la toate măsurile necesare pentru implementare
3. Lipsa revizuirii proceselor de business ale organizaţiei pentru a susţine în întregime capacitățile noului sistem infomatic
4. Insuficiente resurse umane alocate pentru susţinerea proiectului
5. Existența anumitor situații particulare, în care competențele persoanelor din echipa de proiect nu vor fi suficiente pentru desfășurarea în bune condiții a anumitor activități
6. Întârzieri în corelarea rezultatelor proiectului cu cele obţinute în cadrul altor proiecte derulate la nivelul MF
7. Participarea redusă la sesiunile de instruire, generată de programul de lucru / activitățile curente și neprevăzute
8. Întârzieri în implementarea activităților proiectului
9. Scurtarea timpului de realizare a sistemului din cauza unor factori externi (de exemplu contractarea cu întârziere) poate conduce la o soluție incomplet elaborată sau cu erori peste pragul așteptat, cât și la scurtarea, în consecință, a perioadei de testare
10. O perioadă de testare redusă ca timp, ținând seama de complexitatea sistemului, de faptul că activitatea în Trezorerie este fluctuantă, existând vârfuri de sarcină periodice și operațiuni care se întâmplă la intervale mai rare de timp (cum ar fi, de exemplu, închiderile de lună sau de an), poate lăsa anumite cazuri netestate complet, cu riscul de a se manifesta erorile foarte târziu față de momentul implementării
11. Subdimensionarea platformelor hardware, software și de comunicații necesare pentru producție poate conduce la sugrumări ale activității, mai ales în perioadele de vârf (în jurul datei de 15 ale lunii, cand se plătesc salariile în sistemul bugetar și în jurul datei de 25 ale lunii, când se încasează obligațiile fiscale)
12. Contestaţie la procedurile de achiziţie publică

În oferta prezentată, Consultantul va comunica măsurile de eliminare sau reducere, după caz, a riscurilor care ar putea afecta implementarea proiectului (cele menționate mai sus precum și cele noi, identificate de acesta). Consultantul va asigura, în cadrul proiectului, toate resursele necesare eliminării sau reducerii riscurilor identificate. Beneficiarul va răspunde solicitărilor consultantului efectuând activitățile care îi revin pentru diminuarea sau eliminarea riscurilor.

Totodată, în situația identificării, pe parcursul derulării proiectului, a unor riscuri suplimentare, Consultantul și le va asuma și le va gestiona în mod corespunzător, inclusiv din punct de vedere al asigurării resurselor (umane, materiale, financiare, informaționale etc.) necesare eliminării / reducerii acestora.

# Prezentarea contextului și actorilor de business

Trezoreria Statului reprezintă un sistem unitar şi integrat prin care statul asigură efectuarea operaţiunilor de încasări şi plăţi privind fonduri publice, inclusiv cele privind datoria publică, şi a altor operaţiuni ale statului, în condiţii de siguranţă şi în conformitate cu dispoziţiile legale în vigoare.

Din punct de vedere organizatoric, unitățile teritoriale ale Trezoreriei Statului funcționează în cadrul Direcțiilor Generale Regionale ale Finanțelor Publice - aflate în subordinea Agenției Naționale de Administrare Fiscală – fiind coordonate din punct de vedere metodologic de către Direcția Generală de Contabilitate Publică din cadrul Ministerului Finanțelor. Mecanismele, legislația, reglementările în baza cărora sunt derulate operațiunile prin intermediul unităților trezoreriei statului sunt inițiate, avizate sau aprobate de către această direcție.

Operațiunile derulate prin intermediul unităților teritoriale ale trezoreriei statului prezintă un caracter specific - mecanismele fiind diferite de cele derulate prin intermediul instituțiilor de credit - dat fiind faptul că la nivelul acestora sunt deschise conturile de venituri și cheltuieli bugetare ale tuturor instituțiilor publice indiferent de modalitatea de organizare și finanțare, iar operațiunile de încasări și plăți au un pronunțat caracter particular, efectuându-se în baza unor seturi de documente specifice sectorului public (buget de venituri și cheltuieli, deschideri de credite, angajamente bugetare, ordonanțări de plată, etc.). La nivelul unităților Trezoreriei Statului conturile amintite sunt deschise în structura clasificației indicatorilor privind finanțele publice (volumul și cuantumul sumelor derulate prin intermediul acestora fiind considerabil).

La nivelul structurilor de trezorerie se derulează, în principal, activități precum:

1. înregistrarea de operațiuni contabile
2. derularea de operațiuni de plăti și încasări prin conturile de cheltuieli şi de disponibilităţi alte instituțiilor publice / agenți economici / persoane fizice
3. editarea zilnică a balanțelor de verificare, extraselor de cont, rapoartelor şi situațiilor financiare aferente operațiunilor derulate
4. realizarea procedurii de închidere / deschidere zi / lună / an
5. efectuarea salvărilor aferente activității zilnice
6. transmiterea zilnică către sistemul național de raportare FOREXEBUG a datelor privind operațiunile derulate
7. preluarea fișierelor cu informații actualizate din sistemul național de raportare FOREXEBUG

Operațiunile derulate de Trezoreria Statului se desfășoară în baza Ordonanței de Urgență a Guvernului nr. 146/2002 privind formarea și utilizarea resurselor derulate prin trezoreria statului, Republicată, cu modificările și completările ulterioare și a Ordinului Ministrului Finantelor Publice nr. 1235/2003 pentru aprobarea normelor metodologice de aplicare a prevederilor Ordonanței de Urgență a Guvernului nr. 146/2002 privind formarea și utilizarea resurselor derulate prin trezoreria statului cu modificările și completările ulterioare, precum și a altor acte normative/reglementări specifice.

## Serviciul Decontări și Relații cu Sistemul Interbancar de Plăți din cadrul Direcției Generale de Contabilitate Publică

1. Asigură recepționarea și transmiterea instrucțiunilor de plată/încasărilor de mică/mare valoare și intertrezorerii în relație cu unitățile trezoreriei statului și instituțiile de credit;
2. Asigură prelucrarea, verificarea integrităţii, decontarea şi înregistrarea în contabilitatea de decontări a instrucţiunilor de plată electronice de mare şi mică valoare în relaţia trezoreria statului - instituţii de credit, precum şi a instrucţiunilor de plată electronice interjudeţene (intertrezorerii);
3. Asigură înregistrarea în contabilitatea de decontări a instrucțiunilor de debitare/creditare directă ale contului curent general al Trezoreriei Statului realizate de către Banca Națională a României;
4. La nivelul serviciului nu există clienți înregistrați, sunt deschise doar conturi de decontări

## Trezoreria Operativă Centrală din cadrul Direcției Generale de Contabilitate Publică

1. Asigură înregistrarea în conturile corespunzătoare a plăţilor dispuse din conturile de cheltuieli şi de disponibilităţi deschise la nivelul TOC
2. Asigură procesarea ordinelor de plată asupra contului deschis la TOC pe seama Comisiei Europene, editarea extraselor de cont şi colaborarea cu direcțiile de specialitate din cadrul Ministerului Finanțelor în vederea transmiterii către Comisia Europeană a unui mesaj de confirmare a operațiunii
3. Asigură transmiterea ordinelor de plată către SDIRSIP în vederea decontării
4. Asigură înregistrarea în conturile bugetare / disponibilități beneficiare deschise la nivelul său a încasărilor de mică / mare valoare și a celor interjudețene
5. Asigură înregistrarea operațiunilor de debitare / creditare a contului curent general al trezoreriei statului
6. Asigură efectuarea, la nivelul TOC, a operațiunilor privind împrumuturile acordate de către Ministerul Finanțelor în scopuri stabilite prin acte normative, conform normelor metodologice aprobate prin OMF sau HG
7. Asigură derularea operațiunilor necesare transmiterii către conturile bugetare/de disponibilități beneficiare a sumelor încasate de la persoanele fizice prin intermediul contului tranzitoriu deschis pe seama Ministerului Finanțelor la instituții de credit
8. Asigură distribuirea, către unitățile trezoreriei statului, a sumelor ce fac obiectul actelor de executare silită virate de instituțiile de credit în contul deschis special la nivelul Trezoreriei operative centrale, precum și transmiterea către sistemul e-Popriri a informațiilor din documentele de plată;
9. Asigură generarea ordinelor de plată Loteria bonurilor fiscale, încărcarea informațiilor aferente acestora în aplicația informatică precum şi transmiterea spre decontare către SDIRSIP;

## Activitatea de Trezorerie și Contabilitate Publică din cadrul Direcției Generale Regionale a Finanțelor Publice / Administrației Județene a Finanțelor Publice

1. Asigură recepţionarea, verificarea şi înregistrarea contabilă a operațiunilor din fişierele ce conţin plăți de la nivelul unităţilor trezoreriei statului din cadrul judeţului şi crează fişierele pe care urmează să le transmită în vederea decontării către SDIRSIP / unităţilor de trezorerie destinatare din cadrul judeţului, după caz
2. Asigură recepţionarea, verificarea şi înregistrarea contabilă a operațiunilor din fişierele ce conţin încasări prin virament în conturile de venituri / cheltuieli bugetare sau de disponibilităţi, destinate unităţilor de trezorerie din cadrul judeţului, transmise de SDIRSIP şi crează fişierele pe care urmează să le transmită unităţilor trezoreriei statului din cadrul judeţului
3. Alte activități

## Activitatea de Trezorerie și Contabilitate Publică a Municipiului București, Trezoreriile Sectoarelor Municipiului București, din cadrul Direcției Generale Regionale a Finanțelor Publice București

1. Asigură derularea operațiunilor de încasari și plăți în numerar / virament pentru clienții lor, în conformitate cu prevederile legale în vigoare
2. Asigură verificarea şi înregistrarea în cadrul aplicaţiei informatice a instucțiunilor de plată şi creează fişierele pe care urmează să le transmită în vederea decontării la SDIRSIP
3. Asigură recepţionarea, verificarea şi înregistrarea în cadrul aplicaţiei informatice a fişierelor ce conţin încasări prin virament în conturile de venituri/cheltuieli bugetare sau de disponibilităţi, transmise de SDIRSIP
4. Alte activități

## Unități teritoriale ale trezoreriei statului din cadrul Activităților de Trezorerie și Contabilitate Publică din cadrul Direcțiilor Generale Regionale ale Finanțelor Publice / Administrațiilor Județene ale Finanțelor Publice

1. Asigură derularea operațiunilor de încasari și plăți în numerar / virament pentru clienții lor, în conformitate cu prevederile legale în vigoare
2. Transmite/primeşte de la SDONPE din cadrul ATCP containerele cu operaţiuni de plăţi/încasări de mare valoare, mică valoare, intertrezorerii şi intratrezorerii
3. Verifică fişierele cu operaţiuni de plăţi / încasări transmise / primite la / de la SDONPE din cadrul ATCP şi le preia în baza de date a unităţii trezoreriei statului
4. Alte activități

# Descrierea sistemelor informatice existente

În acest subcapitol a fost inclusă o descriere sumară a sistemului informatic TREZOR existent, precum şi a sistemelor cu care acesta interacționează.

În continuare sunt prezentate principalele funcționalități ale acestor sisteme informatice.

## Aplicația TREZOR

Aplicația actuală TREZOR este un sistem informatic descentralizat, în arhitectura client server cu o organizare pe trei niveluri: central (SDIRSIP), județean (ATCP - SDONPE) și operativ, respectiv 202 unități teritoriale operative ale trezoreriei statului (la nivelul municipiilor reședință de județ, a municipiilor, orașelor, comunelor, sectoarelor Municipiului Bucureşti și a Municipiului Bucureşti), o trezorerie operativă centrală (TOC).

Funcționalitățile prezentate în continuare sunt oferite cu titlu de exemplu, gama prestațiilor din contract nu va fi limitată strict la acestea.

### Funcționalități asigurate de aplicația TREZOR

Principalele funcționalități asigurate de aplicația TREZOR sunt:

1. deschidere zi contabilă în aplicația TREZOR
2. integrare cu componenta Nomenclatoare și Registru EP a Forexebug - exportul datelor de la Trezoreria Centrală și importul acestora la nivelul UTTS
3. integrare cu componenta Forexebug DW a Forexebug - exportul datelor aferente bugetelor individuale de la Trezoreria Centrala și importul acestora la nivelul UTTS
4. integrare cu componenta CAB a Forexebug - exportul datelor aferente angajamentelor de la Trezoreria Centrală și importul acestora la nivelul UTTS
5. gestionarea nomenclatoarelor proprii de clienți - instituții publice, operatori economici, ONG-uri, PFA identificate prin CIF, PF identificate prin CNP, etc.
6. gestionarea nomenclatoarelor operaționale (de ex.: utilizatori, conturi, cod operațiuni, tipuri documente, POS, instituții bancare, etc.)
7. gestionare nomenclatoare perioade calendaristice (de ex.: calendar, an curent, luna curentă, perioadă de închidere, etc.)
8. gestionarea altor tipuri de nomenclatoare necesare funcționării aplicației TREZOR (de ex.: acreditive, programe operaționale, evidență conturi de garanție de bună execuție, etc.)
9. gestionarea conturile deschise la Trezoreria Statului
10. gestionarea tranzacțiilor aferente conturilor deschise la Trezoreria Statului
11. deschiderea / blocarea conturilor analitice pentru instituțiile publice, agenți economici, ONG-uri, PFA identificate prin CIF, PF identificate prin CNP, etc.
12. preluare de cereri de deschidere de credite și dispoziții bugetare pentru repartizarea / retragerea de credite bugetare
13. efectuarea operațiunilor de plăți (virament) - preluarea prin scanare (cod de bare) sau manuală a ordinelor de plată individuale și a ordinelor de plată multiple, prezentate de către clienții trezoreriei (instituții publice, agenți economici, etc.) sau întocmite de unitatea de trezorerie
14. preluarea manuală a notelor contabile interne;
15. preluarea manuală/automată/prin scanare a notelor contabile de corecții CAB;
16. preluarea ordinelor de plată multiple electronice (OPME)
17. înregistrarea operațiunilor de încasare de venituri ale bugetului de stat sau venituri cuvenite altor bugete administrate de ANAF, efectuate cu cardul bancar, de către contribuabili persoane fizice și juridice, prin intermediul echipamentelor POS la sediul UTTS și editarea (generarea) de chitanțe / taloane
18. efectuarea de operațiuni în numerar prin:
    1. scanare / preluare manuală a documentelor prezentate de către plătitori sau procesarea datelor pe baza intenției verbale a plătitorilor și editarea (generarea) de chitanțe / taloane (procesare de încasari în numerar)
    2. scanare sau preluare manuală a CEC-urilor prezentate de clienții trezoreriei (procesarea ridicărilor de numerar)
    3. editare de dispoziții de plată pentru restituiri în numerar de impozite, taxe si alte sume
19. efectuarea de validări automate la efectuarea de operațiuni, prin intermediul unor procese / controale automate, ca de exemplu:
    1. verificare cu prevederile din bugetul individual
    2. verificare cu creditele bugetare deschise
    3. verificare cu soldul contului de disponibil / singular / total cont sintetic
    4. nu sunt permise operațiuni între aceleași conturi analitice
    5. la OPTM-uri, OPME-uri, NC corecție CAB, NC corecție CAB online și CEC-uri multiple numărul operațiunilor din document trebuie să coincidă cu numărul operațiunilor scanate / preluate
    6. la OPTM-uri, OPME-uri, NC corecție CAB, NC corecție CAB online și CEC-uri multiple suma totală trebuie să coincidă cu suma operațiunilor scanate / preluate
    7. verificare să nu se completeze codul de angajament, indicatorul de angajament și codul de program bugetar la alte conturi decât cele de cheltuieli
    8. verificare cu disponibilul din CAB
    9. verificare cu angajamentele din CAB
    10. verificarea cu totalul plăților pe anul curent sau pe anul anterior, după caz, la nivel de angajament și indicator angajament
    11. verificare cu codul de program bugetar
20. confirmarea documentelor înregistrate de către persoanele cu atribuții în acest sens
21. Anularea documentelor înregistrate
22. exportul, respectiv importul de fișiere aferente mesajelor de plată / încasare prin virament
23. interconectarea cu aplicația QpayIntegrator, pentru transmiterea / primirea de mesaje de plată în relația cu sistemul interbancar de plăți
24. interconectarea cu aplicația QpayIntegrator, pentru transmiterea de mesaje de informare SWIFT
25. importul de fișiere cu mesaje de plată de la UTTS și ulterior exportul acestor mesaje de plată, grupate pe destinatari, pentru operațiunile interne ale TS (intra și intertrezorerii)
26. calcul cote din impozitul pe venit pentru UAT-uri și preluare note contabile aferente
27. înregistrarea automată a comisioanelor zilnice pentru ordinele de plată întocmite de operatorii economici și persoanele fizice în relația cu sistemul bancar
28. calcul și preluare comisioane lunare
29. gestionarea operațiunilor înregistrate automat în conturile dedicate operațiunilor în curs de lămurire, aferente încasărilor prin SEP – procesarea automată sau manuală a acestora prin notă contabilă sau OPT (retur)
30. preluarea manuală a operațiunilor privind depozitele la termen gestionate prin aplicația DEPTERM, pentru clienții trezoreriei
31. preluarea operatiunilor privind răscumpărările de certificate de depozit gestionate prin aplicația EMICERT, pentru clienții trezoreriei
32. calcularea și preluarea dobânzilor lunare aferente conturilor purtătoare de dobândă
33. calculul automat al dobânzii la data solicitării închiderii contului pentru conturile purtătoare de dobândă deschise pe seama operatorilor economici
34. generarea de rapoarte și situații de verificare specifice
35. gestionarea titlurilor de stat în cadrul Programului Tezaur :
    1. gestiune nomenclatoare emisiuni, clienți, etc.
    2. preluare cereri de deschidere cont de subscriere și editare raport
    3. preluare operațiuni de subscriere și editare formulare de subscriere
    4. anulare operațiuni de subscriere și editare formular de anulare
    5. editare cereri de răscumpărare anticipată, transfer a dreptului de proprietate și transfer către moștenitori și preluare operațiuni
    6. editare notă contabilă operațiuni de subscriere / anulare subscriere / răscumparare anticipată / transfer
    7. preluare automată a răscumpărărilor anticipate și editarea notei contabile
    8. Export / import operațiuni de subscriere / anulare subscriere / răscumpărare anticipată / transfer
    9. Export / import sold conturi de subscriere
    10. Export / import operatiuni de alimentare cu numerar a contului de subscriere și editarea de rapoarte pentru raportarea către ONPCSB
    11. Centralizare cereri de răscumpărare anticipată
    12. Import operațiuni de subscriere / anulare subscriere / răscumpărare anticipată efectuate prin Compania Națională Poșta Română
    13. Gestiune registru investitori
    14. Editare raport situație investitor
    15. Calculul și preluarea dobânzilor
    16. Virarea valorii nominale la scadență în conturile de subscriere
    17. Editare rapoarte cu soldul emisiunilor titlurilor de stat
    18. Preluarea formularelor depuse online și transmiterea de rapoarte către investitorii care le-au depus
36. gestionarea conturilor individuale de economii Junior Centenar:
    1. actualizare clienți și conturi analitice
    2. calcul dobânzi
    3. editare situații raportare
    4. virare sume în conturile deschise la alte trezorerii
37. exportul datelor privind execuția bugetară (rulajele zilnice ale conturilor analitice) din aplicația TREZOR de la nivelul UTTS la Trezoreria Centrala, în vederea replicării datelor în Forexebug - DW (integrare cu componenta ForExeBug - DW)
38. exportul datelor privind operațiunile efectuate pe conturile de cheltuieli din aplicația TREZOR de la nivelul UTTS la Trezoreria Centrala, în vederea replicării datelor în CAB (integrare cu componenta CAB)
39. transfer de date în relația cu organul fiscal:
    1. actualizarea de nomenclatoare proprii de clienți
    2. transmiterea către organul fiscal a operațiunilor zilnice efectuate pe conturile aferente impozitelor și taxelor cu evidență fiscală
    3. preluarea automată a fișierelor de distribuiri, compensări, restituiri prin virament, prin mandat postal, sponsorizări entități non profit, notari, etc.
40. import de date (ordine de plată) generate de alte aplicații informatice, la nivel central (de ex.: mesaje electronice de plată Contul Tranzitoriu, ordine de plată generate de aplicația CashBNR, operațiuni aferente Loteriei Bonurilor Fiscale)
41. operațiuni aferente plăților efectuate prin Sistemul Național Electronic de Plată online
42. preluare automată, prin fișiere de tip DMP, a notelor contabile generate de aplicația TAXEDIV în punctele de încasare și înregistrarea contabilă a tuturor operațiunilor preluate, în aplicația TREZOR
43. operațiuni aferente plăților efectuate în contul unic de popriri de la trezoreria operativă centrală, cu validarea acestora în sistemul ePopriri și distribuirea sumelor la unitățile operative ale trezoreriei statului
44. export / import de date de la nivelul TOC către / din aplicația CREDPRIV
45. preluarea automata de plăți la trezoreria operativă centrală pe baza înregistrărilor transmise din aplicația FTY-STAR
46. înregistrarea și transmiterea confirmărilor universale
47. editarea extraselor de cont, semnarea și transmiterea acestora
48. închidere de zi contabilă
49. operațiuni de întreținere specifice (verificări de coerență a bazei de date, arhivare, salvare, etc.)
50. operațiuni specifice de deschidere an
51. evidența contabilă a operațiunilor în perioada de închidere, atât pe anul curent, cât și pe anul anterior
52. operațiuni specifice de închidere an

### Rapoarte generate din TREZOR

Rapoartele generate de aplicația TREZOR, deși pot fi editate în multiple structuri, sunt rapoarte predefinite elaborate pe baza unor cerințe/criterii fixe, neexistând posibilitatea modificării/customizării acestora în funcție de preferințele utilizatorului. Cu titlu de exemplu:

1. Balanțe analitice și sintetice, zilnice și lunare
2. Jurnale analitice și sintetice
3. Registrul jurnal
4. Registrul jurnal de operațiuni în curs de lămurire și clarificare sume
5. Extrase de cont
6. Extrase de cont pentru convențiile încheiate cu instituții de credit
7. Borderou de încasări şi plăți
8. Note contabile dobânzi şi comisioane lunare
9. Fișe de calcul dobânzi
10. Situația impozitului pe venit, pentru calculul cotelor defalcate aferente UAT
11. Borderou repartizări credite interjudețene
12. Execuție venituri pentru toate bugetele
13. Fișe de cont
14. Bilanț și anexe
15. Cont de execuție
16. Listă operațiuni zilnice

Rapoartele menționate mai sus pot fi editate în multiple structuri. În cadrul acestui proiect se dorește simplificarea, standardizarea și limitarea machetelor de raportare.

### Arhivarea datelor din TREZOR

Pe serverul de producție al fiecarei UTTS, datele se țin în arhive pentru o perioada de 1 - 5 ani, dupa care se transferă pe un server de arhivă.

### Tehnologia TREZOR

Arhitectura client-server

1. Baze de date: Oracle 10g la nivel central, Oracle 8 la nivel județean, municipii, orașe, etc.
2. Interfață: Oracle Forms Builder 5.0.6.11.0, Oracle Reports Builder 3.0.5.10.2
3. Transferul fișierelor de date între noduri (unități operative, trezorerii județene, centrală): se realizează prin aplicația de transmitere containere, dezvoltată intern de MF.

## Aplicația TAXEDIV

Aplicaţia informatică TAXEDIV asigură preluarea încasărilor în numerar și a celor efectuate prin intermediul echipamentelor POS, la nivelul punctelor de încasare ale UTTS, reprezentând o modalitate alternativă pentru efectuarea operațiunilor de încasări de venituri bugetare, și alte sume.

Aplicaţia TAXEDIV permite preluarea manuală / prin scanare a documentelor prezentate de către plătitori sau în baza intenției verbale a plătitorilor, a datelor aferente operațiunilor de încasare a veniturilor bugetare, și alte sume.

La sfârşitul fiecarei zile, după închiderea zilei de lucru, datele referitoare la încasările zilei curente se importa în aplicaţia TREZOR.

### Funcționalități asigurate de aplicația TAXEDIV

1. gestiune nomenclatoare operaționale proprii (de ex.: utilizatori, puncte de încasare, conturi, taxe, clasificație, POS)
2. gestiune nomenclatoare proprii de clienți
3. posibilitate de preluare a chitanței prin citire cod bare sau prin introducere date comunicate de plătitori
4. anularea operațiunilor preluate
5. editarea chitanțelor, înseriate automat, și a talonului pentru încasarea de venituri bugetare, și alte sume
6. confirmarea operatiunii
7. eliberare duplicate chitanțe din arhivă
8. editare rapoarte (de ex. jurnale analitice de încasări și registre de casa)
9. exportul de date aferente operațiunilor derulate în punctele de încasare, în fișiere de tip DMP, pentru importul în aplicația TREZOR
10. operațiuni de întreținere:
    1. deschidere zi contabilă
    2. închidere zi contabilă
    3. salvare date
    4. arhivare date, etc.

### Interconectarea aplicației

1. notele contabile din punctele de încasare sunt preluate în aplicația TREZOR, prin transferuri intermediare / finale ale datelor aferente zilei contabile
2. datele sunt preluate în TREZOR după adaugarea în nomenclatoarele aplicației a conturilor analitice nou create; pentru evidențierea conturilor inexistente, TREZOR editeaza liste de erori aferente acestora

### Sisteme necesare aplicației

1. sistem e-mail pentru transmiterea fișierelor între punctele de încasare și unitatea de trezorerie operativă

## Aplicația de administrare de depozite (DEPTERM)

Aplicația asigură o evidență extracontabilă a depozitelor la termen constituite în trezorerie de către instituțiile publice și operatorii economici.

### Funcționalități asigurate de aplicația DEPTERM

1. deschiderea zilei de lucru
2. gestiune nomenclatoare operaționale proprii (ex.: utilizatori, clienți, conturi, adrese cu procentul de dobândă, etc.);
3. preluarea datelor din convențiile de constituire a depozitelor și editarea notelor contabile și a jurnalelor de constituire;
4. închiderea automata a depozitelor înainte de scadență (la vedere) cu editarea situațiilor aferente;
5. închiderea automată a depozitului la scadență, cu editarea situațiilor aferente;
6. generarea unor raportări (ex.: situaţia depozitelor aflate în sold în ziua curentă, extras de cont pentru depozitele constituite/închise de un client);
7. generare note contabile aferente depozitelor (care ulterior sunt preluate manual în aplicația TREZOR)
8. arhivarea depozitelor închise la scadență sau înainte de scadență;
9. închiderea zilei de lucru

## Aplicația de administrare de certificate de trezorerie (EMICERT-EMIRAP)

### Aplicația EMICERT

Aplicația informatică asigura gestionarea emisiunilor și răscumpărărilor de certificate de trezorerie destinate persoanelor fizice la nivelul unităților operative ale trezoreriei statului.

Utilizatorii aplicației sunt angajați ai unităților operative ale trezoreriei statului având alocate roluri cu atribuții distincte.

#### Funcționalități asigurate de aplicația EMICERT

1. gestiune nomenclatoare operaționale proprii (ex.: utilizatori, clienți, prospecte de emisiune, valori nominale, date calendaristice de vânzare, scadență și depozit, procente de dobânzi la vedere, etc.);
2. înregistrarea operațiunilor de vânzare/răscumpărare a certificatelor de trezorerie sau de depozit;
3. asigurarea evidenței certificatelor de trezorerie transformate în certificate de depozit și calculul dobânzilor cuvenite;
4. generarea notelor contabile aferente certificatelor (care ulterior sunt preluate manual în aplicația TREZOR)
5. generarea raportărilor specifice

#### Interconectarea aplicației

Cu aplicatia EMIRAP: raportările specifice (zilnice și lunare) generate se importa în EMIRAP prin intermediul unor fisiere de tip DMP.

#### Sisteme necesare aplicatiei

Sistem e-mail pentru transmiterea fișierelor către aplicația EMIRAP.

### Aplicația EMIRAP

Aplicația asigură prelucrarea automată a raportărilor de la unitățile de trezorerie către DGTDP privind operațiunile de subscriere și răscumpărare certificate de trezorerie destinate populației.

Utilizatorii sunt angajați ai unităților de trezorerie și DGTDP, grupaţi pe funcţii. Fiecare funcție are rol unic determinat cu acces pe module separate.

#### Funcţionalităţile principale

1. deschiderea zilei de lucru
2. importul datelor raportate
3. centralizarea datelor raportate
4. exportul datelor către DGTDP
5. generarea raportărilor specifice
6. arhivarea înregistrărilor
7. închiderea zilei de lucru

În situația în care preluarea automată a informațiilor, prin import, nu poate fi efectuată, aplicația EMIRAP permite preluarea manuală a acestora.

#### Interconectarea aplicației

EMIRAP se interconecteaza cu aplicația EMICERT, prin importul datelor din fișierele DMP transmise, cuprinzând:

1. informații aferente certificatelor vândute/răscumparate (zilnic)
2. informații aferente certificatelor aflate în sold (lunar)

#### Sisteme necesare aplicației

Sistem e-mail pentru recepționarea fișierelor generate de aplicația EMICERT. În cazul preluării manuale a datelor, este necesară transmiterea acestora printr-un canal de comunicație corespunzător.

## Aplicația CASHBNR

Aplicația asigură preluarea informațiilor referitoare la operațiunile cu numerar ale trezoreriilor în relația cu BNR și cu instituțiile de credit , realizarea de raportări către BNR.

### Funcționalități asigurate de aplicația CASHBNR

1. introducere informații pentru efectuarea operațiunilor de retragere numerar de la BNR, alimentare a conturilor de disponibil deschise la instituțiile de credit pe seama unităților trezoreriei statului fără casă tezaur, depunere de numerar la BNR (depunere însemne monetare bune/uzate și depunere de însemne monetare deteriorate). Informațiile sunt introduse de angajații ATCP Județene/ATCP a MB/sectoarelor MB și sunt confirmate de către angajați ai DGTDP - SONIPD (cu excepția operațiunilor de depunere numerar la BNR, pentru care confirmarea se realizează tot la nivelul ATCP Județene / ATCP a MB / sectoarelor MB).
2. introducere informații privind soldul zilnic / lunar de numerar existent la nivelul județului / sectorului / ATCP a MB (pentru situațiile lunare este furnizată și structura soldului cu detaliere pe cupiuri).
3. generare fișiere XML aferente cererilor de retragere numerar de la BNR, anunţurilor de depunere și situației zilnice/lunare a numerarului existent la nivelul unităţilor trezoreriei statului cu casă tezaur.
4. generare OPT-uri dematerializate aferente cererilor electronice de retragere numerar de la BNR/cererilor electronice de alimentare a conturilor de disponibil
5. generare rapoarte aferente operațiunilor / situațiilor procesate
6. gestionarea stărilor operațiunilor
7. arhivarea zilnică a informațiilor, închidere/deschidere zi

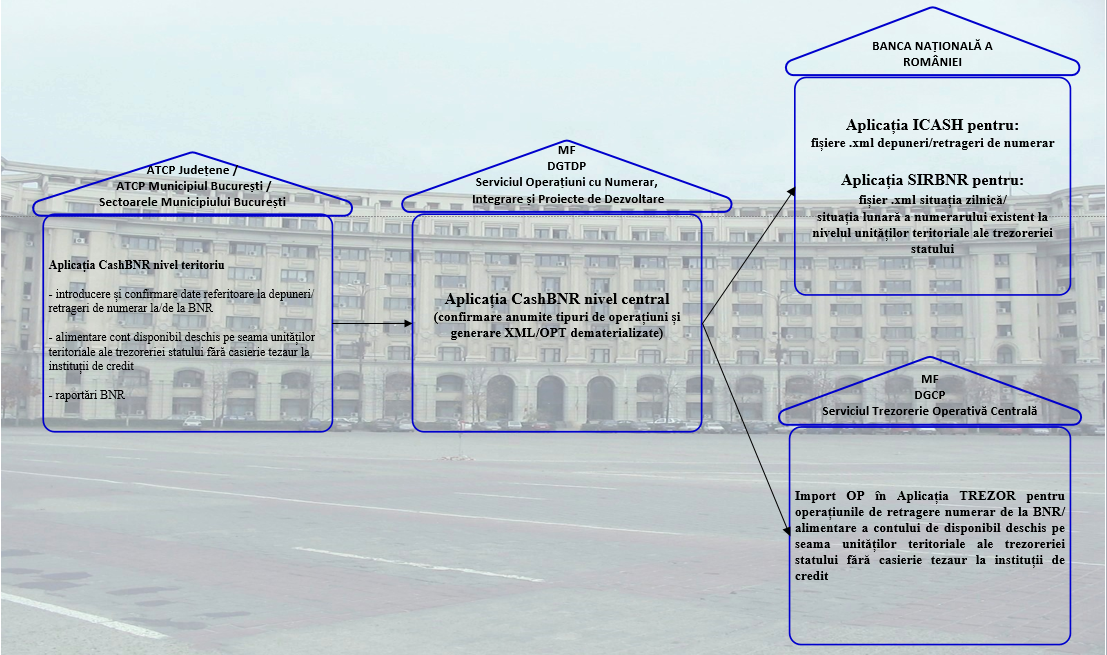
### Interconectarea aplicației CASHBNR

TREZOR (TOC): import informatii în vederea înregistrării acestora în contabilitatea Trezoreriei Operative Centrale și ulterior decontarea instrucțiunilor de plată (achitarea contravalorii numerarului către BNR / institutiile de credit) prin SEP

### Sisteme necesare aplicației CASHBNR

Sistem e-mail pentru transmiterea documentelor (copii scanate) în baza cărora angajații DGTDP - SONIPD realizează confirmarea/verificarea informațiilor introduse în aplicație.

Figura 5 Operațiuni realizate în aplicația Cash BNR



## Aplicația Cont Tranzitoriu

Aplicația asigură recepţionarea şi prelucrarea în sistem informatic a fişierelor electronice de plăţi transmise de instituţiile de credit la nivelul cărora sunt deschise şi funcţionează pe seama MF conturi tranzitorii prin intermediul cărora contribuabilii persoane fizice achită obligaţii către bugetul general consolidat.

### Funcționalități asigurate de Cont Tranzitoriu

1. încărcare fișiere electronice de plăți primite de la instituțiile de credit;
2. validări ale fișierelor/ informațiilor din fișiere;
3. generare coduri IBAN aferente conturilor bugetare/de disponibilități beneficiare in functie de arondarea persoanei fizice pentru care se achită obligația de plată;
4. transferul informațiilor în aplicația TREZOR în vederea înregistrării în contabilitatea TOC;
5. generare fișiere TXT de retur;
6. aplicarea de filtre pentru identificarea tranzacțiilor
7. generare rapoarte
8. gestionare stări aferente tranzacțiilor.

### Interconectarea aplicației Cont Tranzitoriu

1. TREZOR (SDIRSIP): verifică încasarea sumelor de la bănci;
2. TREZOR (TOC): transmitere informații în vederea înregistrării în contabilitate;
3. Registrul General RCNG (baza de date cu CNP-urile persoanelor fizice) – pe baza căruia se obține arondarea fiscală a persoanei fizice pentru care se realizează plata.

### Sisteme necesare aplicației Cont Tranzitoriu

1. Sistem e-mail securizat pentru recepționarea / transmiterea fișierelor electronice de plăți/ fișierelor electronice de retur
2. Aplicație de criptare / decriptare, semnare electronică și verificare semnătură electronică a fișierelor de plăti transmise de către / către instituțiile de credit

## Aplicația de deschideri de credite Dcredite

Aplicația informatică gestionează deschiderile, repartizările și retragerile de credite bugetare din bugetul de stat, bugetul asigurărilor sociale de stat, bugetul asigurărilor pentru șomaj, bugetul Fondului național unic de asigurări sociale de sănătate, depuse la Ministerul Finanțelor.

### Funcționalități asigurate de aplicația Dcredite

1. Actualizarea nomenclatoarelor (utilizate în validarea datelor şi editarea situaţiilor);
2. Preluarea datelor din documentele de intrare:
   1. cereri pentru deschiderea de credite bugetare din bugetul de stat, bugetul asigurărilor sociale de stat, bugetul fondului pentru șomaj și bugetul fondului național unic al asigurărilor sociale de sănătate ;
   2. dispoziții bugetare privind repartizarea creditelor bugetare pentru ordonatorii principali, ordonatorii secundari și ordonatorii terțiari direct subordonați ordonatorilor principali de credite;
   3. dispoziții bugetare privind retragerea creditelor bugetare pentru ordonatorii principali, ordonatorii secundari și ordonatorii terțiari direct subordonați ordonatorilor principali de credite;
   4. situații, dispoziții bugetare privind retrageri/repartizări de credite interjudețene pentru care nu se primesc fișiere, în cazuri de reglări ale execuției bugetare ca urmare a reorganizărilor, etc.
3. Verificarea încadrării în prevederile bugetare și în limitele de cheltuieli, dacă este cazul;
4. Verificarea pe bază de corelații la nivel de capitol, grupă, titlu, alte subdiviziuni de cheltuieli bugetare, după caz;
5. Actualizarea deschiderilor cumulate cu operațiunile preluate;
6. Editarea situaţiilor zilnice (lista deschiderilor și retragererilor de credite bugetare, comunicări privind deschiderile/retragerile de credite bugetare de înștiințare a ordonatorilor, borderouri privind conținutul corespondenței pentru trezoreriile județene, a municipiului București, sectoarelor acestuia și TOC (situația disponibilităților pe indicatori de clasificație funcțională și economică, situația disponibilităților pe ordonatori de credite, etc.);
7. Importul fișierelor de tip TXT generate din Trezor transmise de către trezorerii privind repartizări/retrageri de credite bugetare efectuate de către ordonatorii secundari de credite;
8. Editarea situațiilor de verificare încrucișată cu datele din trezoreriile operative (din ForExeBug);

### Interconectarea aplicației Dcredite

1. Aplicația asigură preluarea automată a datelor din fișierele de tip TXT generate din Trezor transmise de către trezorerii privind repartizări/retrageri de credite bugetare efectuate de către ordonatorii secundari de credite
2. Preluarea de bugete și modificări ale bugetelor din BugetNG

### Sisteme necesare aplicației

Sistem e-mail pentru recepționarea fișierelor generate de aplicația TREZOR.

C.D.C.B., dispoziții bugetare privind repartizarea creditelor bugetare/dispoziții privind retragerea creditelor bugetare

Înregistrare în registre, în fişele de limite, dacă este cazul, verificare documente, preluare date, semnare, ștampilare, scanare, salvare dispoziții bugetare, editare borderouri, pregătire documente, semnare

D.C.P.- B.O.F.D.C.B.

Trezoreriile judeţene, a municipiului Bucureşti,trezoreriile sectoarelor municipiului Bucureşti și T.O.C. – 1 exemplar dispoziţie bugetară şi un exemplar din borderoul privind conţinutul corespondenţei pentru...

O.P.C.- Comunicare privind deschiderea de credite bugetare / comunicare privind retragerea creditelor bugetare

S.C.G.S.- Comunicare privind deschiderea de credite bugetare/ comunicare privind retragerea creditelor bugetare din bugetul M.F.- A.G.

OPC

A.C.P.; D.G.T.D.P.; D.G.S.P.B.; D.G.A.S.; D.G.L.C.P.F.R.N.C.

D.G.P.B.

D.G.P.B.- comunicare privind retragerea creditelor bugetare

## Aplicația de deschideri de credite pentru bugetul trezoreriei statului Dcredite\_BTS

### Funcționalități asigurate de aplicația Dcredite\_BTS

1. Actualizarea nomenclatoarelor (utilizate în validarea datelor şi editarea situaţiilor);
2. Preluarea dispozitiilor bugetare privind repartizarea creditelor bugetare și a dispozițiilor bugetare de retragere a creditelor bugetare
3. Verificarea încadrării în prevederile bugetare;
4. Verificarea pe bază de corelații la nivel de capitol, grupă, titlu;
5. Actualizarea deschiderilor cumulate cu operațiunile preluate;
6. Înregistrarea operațiunilor contabile;
7. Editarea situaţiilor zilnice (dispozițiilor bugetare privind repartizarea/retragerea creditelor bugetare, care ulterior sunt preluate manual în TREZOR);
8. Editarea situațiilor de sfârșit de lună (situația disponibilităților pe indicatori de clasificație economică, situația disponibilităților pe ordonatori de credite);

## Aplicația Ibancls10g

Aplicația gestionează și generează codurile IBAN ale Trezoreriei Statului

### Funcționalități asigurate de aplicația Ibancls10g

1. setare dată curentă a aplicației
2. gestiune nomenclatoare
3. gestiune și generare IBAN-uri
4. realizare rapoarte
5. afișare conturi
6. utilitare de întreținere

### Interconectarea aplicației Ibancls10g

Aplicația se interconecteaza cu aplicația ForexeNomen în vederea folosirii de nomenclatoare pentru generarea conturilor IBAN.

## Alte aplicații informatice

În cadrul MF, aferent activității de Trezorerie, sunt utilizate și alte aplicații informatice (eg. TRZCENTT, EXEFIN, WEBTREZOR, etc), implicate în raportare, gestiunea / evidențierea operațiunilor contabile. Aceste aplicații vor face obiectul activității de analiză, urmând ca sistemul eTrezor sa cuprindă funcționalități echivalente.

## Aplicația de înrolare a utilizatorilor instituții publice și administratori din trezorerie (Înrolare Forexebug)

Aplicatia de înrolare este o aplicație dezvoltată și implementată de CNIF, destinată înrolării administratorilor din trezorerie și a reprezentanților entităților pentru utilizarea funcționalităților sistemului Forexebug.

Administratorii din cadrul unităților teritoriale ale trezoreriei sunt înrolați de către reprezentanți din cadrul DGTCP în baza certificatului digital necalificat și a datelor de identificare.

Reprezentanții entităților sunt înrolați de administratorii din cadrul unităților teritoriale ale trezoreriei la care sunt arondate entitățile respective, în baza certificatului digital calificat și a datelor de identificare, la funcționalitățile Sistemului Național de Raportare-Forexebug (vizualizare rapoarte generate, transmitere documente electronice, acces la aplicația CAB și vizualizare informații din aplicația CAB). Accesul reprezentanților entităților la aceste funcționalități este securizat și se realizează doar pe baza certificatului digital calificat înregistrat în sistem.

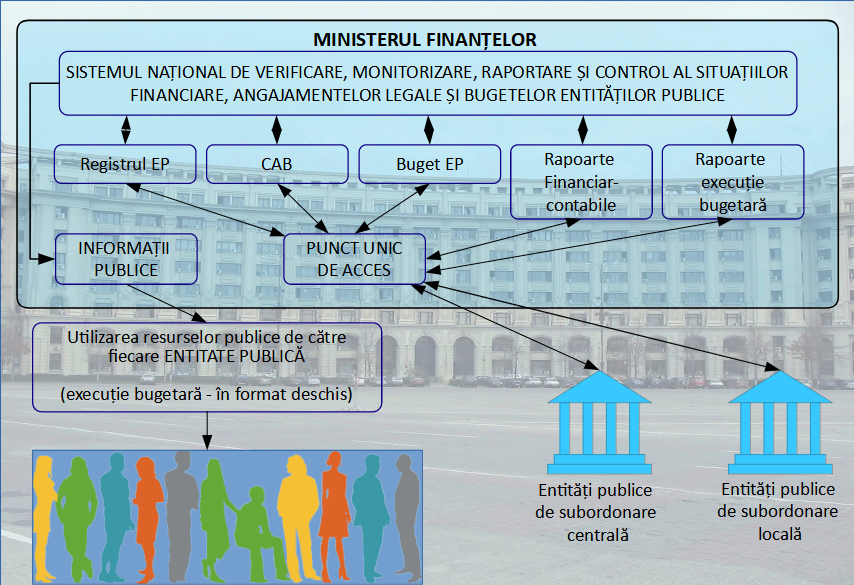
## Sistemul FOREXEBUG

Sistemul naţional de raportare Forexebug contribuie la îmbunătăţirea managementului fondurilor publice şi creşterea eficienţei administraţiei publice centrale şi locale şi a transparenţei administrative, prin cunoaşterea în timp real a informaţiilor de detaliu privind alocarea, angajarea şi utilizarea fondurilor publice, pe subdiviziunile clasificaţiei bugetare, atât la nivel de detaliu, cât şi la nivel agregat pe diferite paliere.

Sistemul oferă ordonatorilor de credite acces la rapoartele de execuţie bugetară proprii şi ale ordonatorilor de credite din subordine, precum şi la extrasele conturilor deschise la unităţile trezoreriei statului. Totodată, sistemul elaborează situaţiile financiare individuale şi centralizate/consolidate ale ordonatorilor principali de credite şi oferă acces la rapoartele introduse în sistem de către ordonatorii de credite din subordine.

Sistemul naţional de raportare Forexebug îi oferă cetăţeanului o mai bună informare în relaţia cu sectorul public, referitor la utilizarea fondurilor publice.

Figura 8 Sistemul național de raportare FOREXEBUG



### Punctul Unic de Acces – Portal ForExeBug

1. reprezintă componenta web a ForExeBug, accesibilă atât public, cât și pe bază de credențiale (certificat digital calificat), integrată cu portalul MF.
2. permite / facilitează publicarea de rapoarte generate de sistem
3. include o secțiune de informare privind sistemul ForExeBug

### Sistemul National de Mesagerie (ForexeSNM)

Aplicația ForexeSNM se prezintă ca o interfață online pentru vizualizarea și descarcarea documentelor generate de sistemele Dedoc și Forexebug.

Pentru a putea utiliza aplicația ForexeSNM, utilizatorii trebuie să se autentifice pe bază de certificat digital calificat înregistrat în prealabil la unitățile teritoriale ale trezoreriei statului.

Utilizatorii pot avea acces la următoarele categorii de rapoarte generate:

1. rapoarte de execuție
2. rapoarte situații financiare
3. notificări
4. rapoarte generale
5. extrase de cont
6. facturi electronice

### DEDOC - Platforma electronica de depunere documente

Platforma electronică de depunere documente (DEDOC) este un sistem de registratură care asigură preluarea uniformă pentru toate tipurile de declaraţii/formulare pe care MF trebuie să le colecteze de la cetăţeni, societăţi comerciale sau instituţii publice.

Sistemul DEDOC are o arhitectura flexibilă care permite extinderea sa prin definirea de noi tipuri de formulare electronice și adaugarea de noi utilizatori. Initial sistemul DEDOC asigura doar preluarea declaratiei D112. Până în prezent, au fost implementate formulare PDF inteligente pentru transmiterea profilului EP, pentru raportarea situațiilor financiare, pentru transmiterea de Bugete Agregate (Administrație Publică Locală) si Buget Individual, pentru transmiterea ordinelor de plată multiple electronice (OPME), a notelor contabile corecție CAB-online, a facturilor electronice, precum și pentru activități suport (preluare în bloc Angajamente Bugetare, solicitare rapoarte, validare rapoarte). Sistemul DEDOC asigură funcționalități de validare a formularelor electronice.

Formularele PDF inteligente asigură o serie de funcționalități, ca de exemplu:

1. export / import date în format XML, pentru fiecare tip de formular
2. validare date la nivel de formular

### Nomenclatoare generale (ForexeNOMEN)

Aplicația ForexeNOMEN se prezintă ca o interfață online pentru gestionarea Nomenclatoarelor Generale, a Registrului Entitatilor Publice, pentru generarea și întreținerea de matrici (MCVB, COFOG3, etc), pentru gestionarea obligațiilor de raportare, frecvente și calendar depuneri, validarea manuala a formularelor.

Aplicația oferă interfață online de monitorizare și auditare a informatiilor din aplicație, precum și generare de rapoarte specifice.

### Aplicatia Control Angajamente Bugetare (CAB)

1. aplicația CAB se prezintă ca o interfață online pentru gestionarea Angajamentelor Bugetare pe tot ciclul de viață al acestora.
2. aplicația asigură procesarea tranzacțiilor de execuție bugetară provenite din TREZOR. Aplicația este integrată cu ForexeNOMEN pentru Nomenclatoare Generale, cu DEDOC pentru preluare în bloc Angajamente Bugetare, cu ForExeBug pentru preluare Bugete Individuale și stările de „Blocaj” și cu TREZOR pentru transmiterea informațiilor privind angajamentele
3. oferă funcționalități de management și controlul încadrării în prevederile bugetare a utilizării fondurilor publice
4. permite monitorizarea și gestionarea în timp real a angajamentelor bugetare și legale ale entităților publice
5. pe baza datelor înregistrate în CAB de entitățile publice, aplicația verifică atât încadrarea angajamentelor legale și bugetare în bugetul aprobat, cât și încadrarea plăților dispuse în limita angajamentelor încheiate și a recepțiilor efectuate
6. asigură informații privind utilizarea resurselor bugetare la nivelul individual al entității publice și la nivelul ordonatorului principal de credite

### Raportare bugete

1. asigură verificarea bugetelor individuale introduse în sistem de entitațile publice cu bugetul agregat al ordonatorului principal de credite
2. permite validarea plăţilor efectuate din conturile deschise la trezoreria statului în raport cu prevederile bugetului individual

### Raportare situații financiare

1. permite obținerea situațiilor financiare individuale (bilanțul, contul de rezultat patrimonial, fluxul de trezorerie, anexe la situațiile financiare și alte rapoarte individuale)
2. permite obținerea de situații financiare agregate și consolidate la nivel de ordonator principal de credite, pe baza balanțelor de verificare și a rapoartelor introduse de entitățile publice în sistem în format electronic, standardizat, securizat
3. sistemul informatic efectuează validări și reconcilieri cu date din sistem, astfel încât să fie furnizate informaţii de încredere pentru uzul intern al MF, al instituţiilor publice, al altor instituţii abilitate şi a publicului

### Raportare execuție bugetară

1. permite obținerea de informații și rapoarte la nivel de detaliu (COFOG3)
2. permite obținerea de rapoarte agregate și consolidate, privind operațiunile de plăți și încasări derulate de entitățile publice
3. datele obţinute vor fi utilizate pentru analize și rapoarte multicriteriale şi pe serii de timp
4. informatiile și rapoartele pot fi puse la dispoziția entităților publice și a publicului larg, prin intermediul unui sistem informatic dedicat

### Depozitul central de date (ForExeBug DW)

1. asigură stocarea informațiilor provenite din diferite surse de date (TREZOR, ForexeNOMEN, CAB, Dedoc, etc.)
2. organizează informațiile stocate pe dimensiuni în vederea generării de rapoarte multicriteriale și pe serii de timp

### Generarea rapoartelor standard și ad-hoc de către sistemul național de raportare ForExeBug

1. asigură generarea de rapoarte predefinite
2. gestionează dimensiunile utilizate pentru generare de noi rapoarte
3. asigură mecanisme de configurare și generare de noi rapoarte

## Spațiul Privat Virtual

SPV constă în punerea la dispoziţia persoanelor fizice, persoanelor juridice şi altor entităţi fără personalitate juridică a unor servicii electronice în relatia cu Ministerul Finanţelor / Agenţiei Naţionale de Administrare Fiscală. Prin intermediul acestuia se efectuează comunicarea electronică între Ministerul Finanţelor / organul fiscal central şi persoanele fizice, persoanele juridice sau alte entități fără personalitate juridică în legătură cu situaţia financiară sau fiscală a acestora.

## Descrierea infrastructurii de retea a MF/ANAF

Sistemul informatic MF/ANAF utilizează o infrastructură de rețea de date organizată astfel:

1. Nivel 1: Nivel central, localizat în două Centre de date, Centrul Primar (CNIF) din București și Centrul Secundar de date aflat la o distanță de 200 km
2. Nivel 2: Nivel teritorial, localizat în reședințele de județ și în sectoarele din București
3. Nivel 3: Nivel teritorial, localizat în municipii/ orașe/ comune

UTTS funcționează, fie, în sediile de nivel 2 și 3 împărțind cu serviciul fiscal rețeaua de date, fie în sedii independente, ce sunt asimilate, din punct de vedere rețea de date, unor sedii nivel 2 sau 3.

Locațiile ANAF de nivel 2 și 3 se conectează redundant, prin rețeaua intranet, la nivelul central folosind câte doua conexiuni (bucle locale) achiziționate de la operatorii de telecomunicații din piață sau puse la dispoziție de către STS. Conexiunile de buclă locală sunt conectate în infrastructura națională, redundantă, de transport a STS. Benzile de comunicație în rețeaua de date ANAF sunt cuprinse la nivelul 3 între 2Mbps și 10Mbps, la nivelul 2 între 50 Mbps și 100 Mbps și la nivel central de 10Gbps. Fluxurile de comunicatie sunt configurate într-o arhitectura de tip arborescent, astfel încât comunicația între componente se realizează numai printr-un punct comun, unde se aplică reguli și permisiuni de acces la nivel de IP/ clasă de IP-uri.

Echipamentele de comunicație din rețeaua de date MF/ANAF nu beneficiază în general de servicii de întreținere sau asistență tehnică și nici de suport la producător (excepție echipamentele router din locațiile de nivel 2). Astfel, actualizările software, rezolvarea bug-urilor de programare sau înlocuirea în caz de defecțiune nu reprezintă o opțiune în cazul unei avarii.

Pentru sediile de nivel 3, echipamentele de comunicație tip router au fost achiziționate în anul 2005, și prezintă un stadiu avansat de uzură fizică și morală, capacitatea acestora de procesare trafic fiind limitată. Aceste sedii nu beneficiază de echipamente de comutare date (switch-uri) cu posibilități de administrare.

Sediile de nivel 2 utilizează routere achiziționate în anul 2010 care au capacitate de procesare a traficului actual. În aceste sedii există (parțial) echipamente de comutare date (switch-uri) cu posibilități de administrare.

În fiecare din centrele de date ANAF, comunicația cu sediile naționale este agregată prin câte 2 echipamente tip router achiziționate în 2019, care beneficiază de porturile cu viteză de 10 Gbps.

Sediile UTTS ce funcționează independent sunt în numar de 16 locații, din care 7 locații sunt în București (în fiecare sector plus sediul aferent Municipiului București) și 9 locații la nivel național. Aceste locații utilizează infrastructura de rețea de date uzată fizic și moral, cu o vechime de peste 12 ani, aceste sedii fiind în imposibilitatea de a beneficia de avantajele date de noile tehnologii și lățimile mari de banda disponibile în acest moment. În aceste sedii routerele au o capacitate de procesare redusă (maxim 7Mbps trafic criptat agregat per echipament), iar switch-urile au porturi 10/100 Mbps și prezintă discontinuități în funcționare (blocări, restart-uri). De asemenea, deși există câte doi provideri de comunicații per locație, redundanța conexiunilor acestor sedii nu poate fi asigurată corespunzător, deoarece nu există câte două echipamente tip router per locație.

## Descrierea sistemului de balansare aplicații cu F5 Networks

Nivelul de optimizare și securitate a aplicațiilor web este deservit de soluția F5 Networks, BIG-IP, instalată în fața aplicațiilor pe mai multe niveluri. Soluția este compusă din mai multe componente care rulează pe un hardware dedicat:

1. Modul de balansare și optimizare a aplicațiilor web
2. Modul de protecție împotriva atacurilor la nivel de aplicație web
3. Modul de autentificare a utilizatorilor
4. Modul de virtualizare pentru echipamentele F5
5. Modul de protecție și gestionare a serviciilor de DNS
6. Modul de management și integrare cu servicii de tip cloud

**Modulul de balansare și optimizare a aplicațiilor web** este responsabil cu terminarea conexiunilor de la client și deschiderea conexiunilor noi spre serverele de aplicație. Prin acest modul se oferă funcționalitățile de bază cum ar fi balansarea și persistența conexiunilor TCP, precum și funcționalități avansate de manipulare a traficului (inserare headere, modificări în timp real pe conținutul răspunsurilor trimise către clienți, redirectări sau balansări pe bază de conținut în cererea clientului, etc.). Modulul de balansare permite definirea de politici de balansare prin care cererile clienților sunt trimise către diferite servere pe baza informațiilor din cererea clientului (URI, headere, continut XML, etc).

Modulul de balansare și optimizare a aplicațiilor web se află pus în fața tuturor aplicațiilor web, interne sau externe, și datorită modulului de virtualizare acesta poate fi pus independent între mai multe niveluri de aplicație (baze de date, servere de aplicații, servere de portal, etc.). Datorită hardware-ului performant modulul de balansare și optimizare a aplicațiilor web este configurat cu funcționalitatea de SSL offloading pentru toate aplicațiile web care suportă SSL și este responsabil de algoritmii și metodele de criptare negociate pe conexiuni. Pentru aplicatiile care nu suportă conexiuni SSL, modulul permite conexiunile respective într-un mod nesecurizat.

**Modulul de protecție împotriva atacurilor la nivel de aplicație web** este activat pe serviciile web expuse în Internet. Acest modul este responsabil cu asigurarea protecției pentru aplicații web, precum și detectarea atacurilor de tip DoS la nivel de aplicație. Modulul suportă definirea de politici de securitate independente pentru fiecare aplicație în parte, definirea de profile pentru conținut de tip XML/JSON/AJAX, posibilitatea de a defini granular politica de securitate la nivel de URL-uri, headere, parametri, tipuri de fișiere, seturi de caractere. De asemenea permite identificarea atacurilor pe bază de semnături furnizate de către producător sau definite de către utilizatori.

Modulul de protecție împotriva atacurilor la nivel de aplicație web permite identificarea sesiunilor făcute de către programe automatizate sau boți, permite identificarea atacurilor DoS de la acestea, precum și mitigarea lor folosind diferite metode. Pentru atacurile DoS modulul permite detecția pe baza monitorizării TPS-urilor către servere, precum și prin monitorizarea încărcării dinamice a serverelor ce deservesc aplicațiile.

Modulul de protecție împotriva atacurilor la nivel de aplicație web dispune de o funcționalitate de tip „IP Intelligence” ce permite filtrarea atacurilor pe baza unui blacklist furnizat dinamic de către producător.

**Modulul de autentificare a utilizatorilor** este responsabil cu autentificarea utilizatorilor atunci cand accesează resurse protejate și efectuarea de single sign on în serverele de aplicație folosite. Mecanismele de autentificare folosite sunt: utilizator și parolă, certificate digitale și http basic authentication. Modulul suportă autentificări multiple prin implementarea mecanismului de one-time password pentru utilizatorii autentificați. De asemenea modulul permite autentificarea cu certificate digitale client și validarea acestora folosind protocolul OCSP pentru mai multe autorități de certificare și validarea utilizatorului folosind servere LDAP/AD. Toate informațiile despre utilizator necesare aplicației pot fi transmise fie prin mecanisme de SSO în sistemul de autentificare al aplicației fie folosind headere și cookie-uri customizate la nivel de HTTP. Modulul de autentificare este responsabil și pentru restricționarea accesului doar la aplicațiile la care utilizatorul are acces. Aplicațiile pot fi expuse direct printr-un serviciu web sau dacă utilizatorul are acces la mai multe aplicații acestea pot fi expuse folosind un portal.

Modulul de autentificare a utilizatorilor permite implementarea unui IdP (Identity Provider) și SP (Service Provider) pentru implementarea unor mecanisme de SSO (Single Sign On) pentru aplicații externe sau folosind provideri de autentificare externi. Modulul suportă acest lucru folosind SAML sau OAuth, ambele cu mai multe mecanisme de autentificare a utilizatorului.

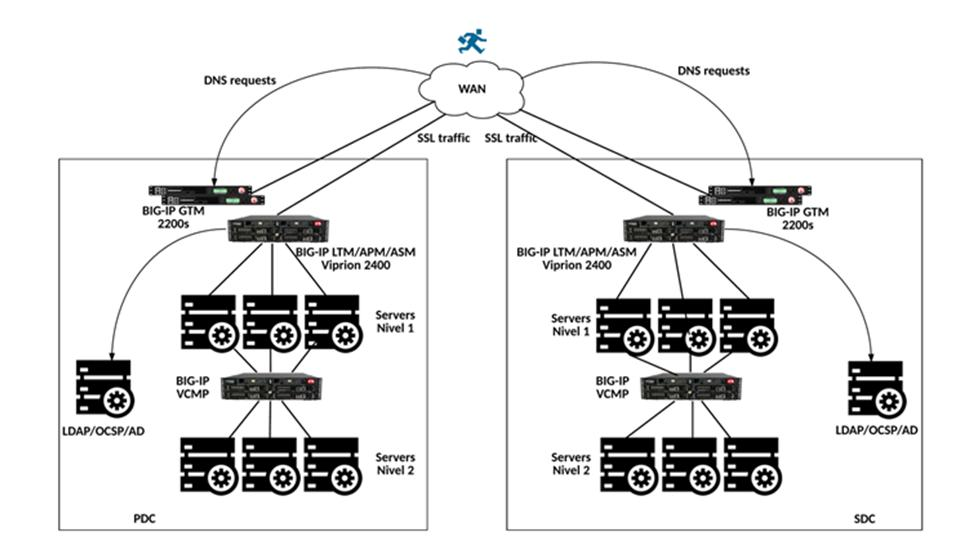
**Modulul de protecție și gestionare a serviciilor de DNS** este responsabil cu protecția și managementul zonelor de DNS interne sau externe, precum și cu balansarea conexiunilor de client către unul din cele două centre de date utilizate prin manipularea răspunsurilor de DNS trimise către clienți. Modulul este responsabil cu monitorizarea disponibilității aplicațiilor web în fiecare centru de date, atât intern cât și extern, permite definirea modului de folosire a aplicațiilor din fiecare centru de date, dinamic sau static, precum și modul de balansare a clienților pe fiecare centru de date: pe bază de adrese IP, geolocation, etc.

Modulul de protecție și gestionare a serviciilor de DNS este responsabil cu administrarea zonelor de DNS expuse intern sau în Internet. Aplicațiile care au nevoie să folosească resursa activă instalată în mai multe centre de date pot folosi acest modul pentru determinarea centrului de date activ.

Toate modulele instalate pe hardware F5 suportă management și integrări cu soluții de tip cloud folosind servicii de tip RestAPI direct către modulul în cauză sau prin platforma de cloud management. *Platforma de cloud management* permite integrarea cu sisteme de orchestrare și automatizare a instalării de aplicații prin definirea unor aplicații disponibile către aceste sisteme. Orice sistem de orchestrare și automatizare poate face instalarea automată a unei configurații de aplicație pe sistemele F5 administrate folosind API-ul disponibil pe platformă. Modulul se integrează cu sisteme de genul Cisco ACI sau Vmware NSX, precum și cu o multitudine de mecanisme de automatizare (Puppet, Chef, Ansible, etc.).

În *Figura 10* este prezentată o diagramă generică pentru arhitectura folosită:

Figura 10 Diagrama generică pentru arhitectura F5



## Descrierea serviciului de management al identității și control acces TIM/TAM

Managementul Identităţii este sistemul informatic unic, implementat pe platforma informatică MF pentru identificarea utilizatorilor şi permiterea accesului la aplicaţiile informatice centralizate (portalizate) – **intranet, extranet** - ale Ministerului Finanţelor.

1. Tivoli Identity Manager - asigură propagarea atributelor unei persoane pe toate directoarele în care o persoană are conturi de utilizator.

Managementul identităţii funcţionează în strictă legătură cu aplicaţia de evidenţă a resurselor umane din cadrul organizaţiei. În cazul MF, ANAF - sistemul informatic de gestiune a resurselor umane este sistemul ONIX, care stochează informaţii privind structura organizaţională a MF, ANAF, AVR, ONAC, personalul efectiv angajat, locul angajării în cadrul organizaţiei, funcţia acestuia.

Informaţiile privind personalul se introduc şi se actualizează pe criteriile de competenţă potrivit legii. Fiecărui angajat din cadrul organizaţiei îi este atribuit un identificator (ID). Identificatorul atribuit este o secvenţă de 8 caractere numerice, generate automat, fără semnificaţie. Acest identificator constituie elementul de legătură dintre sistemul informatic ONIX şi Managementul Identităţii.

Pe baza datelor venite de la HR din sistemul informatic ONIX, în TIM se creează identităţi noi sau se actualizează cele existente, noile informaţii vor fi transmise apoi către toate directoarele gestionate prin platforma de Management al Identităţii: SAM, AD, OID, etc.

**Drepturile de acces**

În sistemul Managementul Identităţii drepturile de acces se dau sub formă de roluri. Un utilizator poate avea unul sau mai multe roluri în funcţie de aplicaţiile la care are acces.

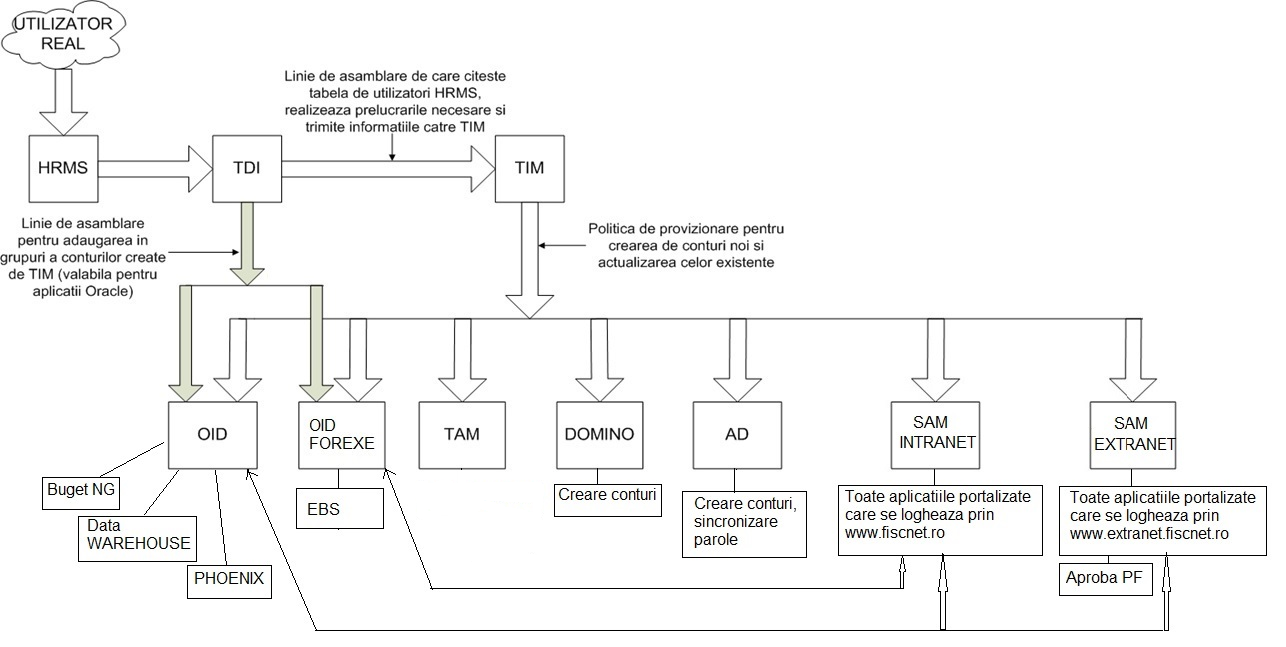
Funcțiile necesare sunt:

1. Furnizează conturi de utilizator persoanelor autorizate pe una sau mai multe resurse la care sunt conectate adaptoarele Tivoli Identity Manager
2. Facilitează utilizatorului posibilitatea de a-şi schimba singur parola pentru conturile ataşate acestuia în sistemul de Management al Identităţii
3. Păstrează contul utilizatorului și datele organizaționale într-un server al directorului LDAP
4. Tivoli Directory Integrator

Tivoli Directory Integrator asigură partea de conectivitate și interacțiunea cu o multitudine de surse de date ce se doresc integrate, indiferent de API-ul fiecăreia, protocol, transport sau format. În loc să lucreze pe partea de date, TDI se concetrează la nivel informațional în partea de transformări, filtrări și alte fluxuri logice pentru fiecare pachet de date ce se dorește integrat.

Cu Tivoli Directory Integrator se pot face librării de soluții de integrare și fluxuri logice ce pot fi folosite ca bază de plecare sau direct în problemele de integrare viitoare.

*Figura 11 Schema flux TIM*



Utilizatorii au acces în sistemul informatic al MF/ANAF, diferențiat pe categorii:

1. Intranet – utilizatori interni MF şi ANAF - [www.fiscnet.ro](http://www.fiscnet.ro);
2. Extranet – instituţiile publice- [www.extranet.fiscnet.ro](http://www.extranet.fiscnet.ro);
3. Internet – contribuabili, persoane fizice şi juridice- [www.mfinante.ro](http://www.mfinante.ro) și [www.anaf.ro](http://www.anaf.ro).

Soluția pentru managementul identității este implementată, în funcție de contextul de portal, astfel:

1. Pentru contextul de portal EXTRANET folosind produsele software:
   1. IBM Security Access Manager (IBM Security Access Manager for Web vers. 7.0), Tivoli Directory Server (IBM Directory Server - 64 bit 6.3.0.17) și Tivoli Identity Manager pentru provizionarea utilizatorilor care se autentifică cu username și parolă
   2. IBM Security Access Manager, Tivoli Directory Server pentru provizionarea utilizatorilor care se autentifică cu certificat digital. Există aplicații dezvoltate pentru înregistrarea utilizatorilor, aplicații care provizionează serverele de TDS și SAM și se leagă și cu serviciile web ale autorităților de certificare.
2. Pentru contextul de portal INTRANET folosind produsele software:
   1. IBM Security Access Manager, Tivoli Directory Server și Tivoli Identity Manager. Conturile utilizatorilor sunt în Microsoft Active Directory, Tivoli Identity Manager-ul provizionează AD-ul, autentificarea în portal se realizează folosind TDS, autorizarea se realizează folosind SAM, contul cu care se autentifică în portal este același cu contul de AD.
3. Pentru contextul de portal INTERNET folosind produsele software:
   1. IBM Security Access Manager, Tivoli Directory Server. Există aplicații dezvoltate pentru înregistrarea utilizatorilor, aplicații care provizionează serverele de TDS și SAM.

Din punct de vedere al modalității de autentificare se folosește:

1. autentificare simplă – nume utilizator/parolă pentru contextele de portal Intranet, Extranet instituții publice
2. autentificare cu doi factori – nume utilizator/parolă/răspuns generat (cod OTP – one time password) și transmis prin mijloace electronice alternative (e-mail) pentru contextul de portal internet, serviciul SPV
3. infrastructura PKI cu certificate digitale:
   1. Calificate – pentru contextul Internet și Extranet
   2. Necalificate – emise de autoritatea de certificare internă a ANAF – în contextul Extranet (platforme pentru autentificare mașină la mașină, Schimb masiv de date)
4. mecanisme standard bazate pe folosirea protocolului OAUTH ca soluție de autorizare a accesului la serviciile de tip API, dezvoltate de MF/ANAF.

De asemenea, există informații și aplicații expuse fără autentificare, disponibile utilizatorilor neautentificați.

## Descrierea situației actuale la nivelul Beneficiarului

Informațiile de mai jos sunt prezentate cu următoarele scopuri:

1. înțelegerea infrastructurii fizice în care vor fi integrate produsele livrate;
2. înțelegerea tehnologiilor cu care produsele ofertate trebuie să se interconecteze;
3. oferirea informațiilor necesare pentru Operatorii economici care optează pentru extinderea tehnologiilor existente.

Activitățile se vor desfășura în Centrele de date ale MF. Centrul Primar de Date (CPD) este localizat în București, iar Centrul Secundar de Date (CSD) este localizat la aproximativ 200 km față de CPD.

Ambele Centre beneficiază de următoarele dotări:

1. Alimentare din două surse diferite de energie electrică, parțial redundante, pentru alimentarea echipamentelor cu cel puțin două surse de alimentare. Acestea sunt: sursa de alimentare neîntreruptibilă (UPS) și rețeaua asistată de grupul electrogen;
2. microclimat stabil (22oC ± 3oC, umiditate 50% ±10%, presiune aer mai mare decât cea din exteriorul spațiului tehnic pentru împiedicarea pătrunderii prafului) pe toată perioada anului;
3. sisteme de avertizare și stingere a incendiului, bazate pe gaz inert.

Ambele Centre de date găzduiesc cabinete metalice (rack-uri) de maxim 42U conectate la rețeaua duală de alimentare cu energie electrică. Următoarele rack-uri de comunicații vor fi utilizate în cadrul proiectului:

1. Centrul Primar de Date:
   1. Rack-ul #1:
      1. Model: Vertiv VR3350;
      2. 23 unități „U” disponibile;
      3. o unitate PDU cu 36 conectori C13 și 3 conectori C19 disponibili;
      4. o unitate PDU cu 36 conectori C13 și 6 conectori C19 disponibili.
   2. Rack-ul #2:
      1. Model: Vertiv VR3350;
      2. 22 unități „U” disponibile (19 adiacente + 3 adiacente);
      3. 2 unități PDU, fiecare cu câte 36 conectori C13 și câte 3 conectori C19 disponibili.
2. Centrul Secundar de Date:
   1. Rack-ul #3:
      1. Model: Vertiv VR3350;
      2. 12 unități „U” disponibile;
      3. 2 unități PDU, fiecare cu câte 30 conectori C13 și câte 3 conectori C19 disponibili.
   2. Rack-ul #4:
      1. Model: Vertiv VR3350;
      2. 12 unități „U” disponibile (19 adiacente + 3 adiacente);
      3. 2 unități PDU, fiecare cu câte 30 conectori C13 și câte 3 conectori C19 disponibili.

Informațiile relevante pentru prezentul proiect, care descriu situația existentă privind interconectarea dintre Centrele de date CPD și CSD, se regăsesc în diagrama următoare:



Cablarea este de tip structurat cu canal de cabluri suspendat. Canalul de cablu acoperă necesitățile ambelor săli. Acest canal va fi folosit la realizarea conectivității fizice a echipamentelor achiziționate în conformitate cu acest caiet de sarcini.

**Notă importantă**: resursele existente descrise în cadrul cap. 5.16 si subcapitolele aferente acestuia sunt valabile la momentul elaborării Caietului de sarcini. Din cauza evoluției Sistemului informatic al MF, este posibil ca la momentul publicării prezentului Caiet de sarcini, resursele disponibile și arhitectura să fie diferite.

### Servere pentru SGBD

Echipamentele dispun de următoarele caracteristici principale:

1. Fiecare server este dotat cu 4 procesoare Intel Xeon Gold 6244;
2. Caracteristici procesor:
   1. frecvența de bază: 3,60 GHz;
   2. frecvența turbo: 4,40 GHz;
   3. 8 nuclee/16 thread-uri;
   4. 24,75 MB Level 3 cache.
3. 512 GB memorie RAM tip DDR4 ECC 2667MT/s;
4. stocare internă: 2xSSD 480 GB, 512n;
5. 2 adaptoare dual port 10 Gbps Ethernet, cu suport PXE 2.0, TCP/IP Offload Engine (TOE), auto-negotiation, Wake-on-LAN, NIC Teaming - load balancing and failover (LBFO);
6. 2 adaptoare dual port 32 Gbps FC HBA echipate cu module optice de tip short-range;
7. 2 adaptoare InfiniBand dual port 100 Gbps QSFP28

### Infrastructura de comunicații InfiniBand

Serverele pentru SGBD (Dell EMC PowerEdge R940) sunt conectate la 4 switch-uri InfiniBand model SB7800 (2 buc. în CPD și 2 buc. în CSD). Fiecare switch este echipat cu 36 porturi QSFP28, care funcționează bidirecțional la 100 Gbps.

### Infrastructura de stocare

Infrastructura de stocare existentă este alcătuită din două echipamente de stocare Dell EMC PowerMax 8000 cu următoarele caracteristici:

1. Centrul Primar de Date: echipamentul de stocare este echipat cu 10 controllere active, 10 TiB memorie cache globală, 415 TB capacitate de stocare utilă in RAID 6, respectiv 830 TB capacitate de stocare utilă efectivă în RAID 6 prezentabilă către host-uri în urma deduplicării și compresiei datelor inline cu un raport garantat de 2:1. Echipamentul de stocare este echipat cu 77 de module NVME flash de capacitate 7,68 TB fiecare, din care 5 sunt pentru hot spare, având libere 103 sloturi NVME pentru capacitate de stocare adițională. Echipamentul dispune de 40 de porturi FC 32 Gbps echipate cu transceivere SFP și 40 de porturi 10 Gbps Ethernet echipate cu transceivere SFP. Porturile sunt distribuite în mod egal pe fiecare dintre controllerele echipamentului de stocare. În configurația existentă, echipamentul asigură o performanță de 900 IOPS per TB util prezentabil către host-uri cu deduplicare inline si compresie inline activate pentru workload de tip 70% acces random, 30% acces secvențial, 50% Read, 50% Write cu IO-uri de dimensiune de 32 KB. Echipamentul de stocare din CPD se replică asincron/sincron cu cel din CSD prin SRDF. Echipamentul de stocare existent permite update de software, firmware fără restartarea controllerelor și este scalabil la 16 controllere și 16 TiB memorie cache globală.
2. Centrul Secundar de Date: echipamentul de stocare este echipat cu 10 controllere active, 10 TiB memorie cache globală, 277 TB capacitate de stocare utilă in RAID 6, respectiv 533 TB capacitate de stocare utilă efectivă în RAID 6 prezentabilă către host-uri în urma deduplicării și compresiei datelor inline cu un raport garantat de 2:1. Echipamentul de stocare este echipat cu 101 de module NVME flash de capacitate 3,48 TB fiecare, din care 5 sunt pentru hot spare, având libere 79 sloturi NVME pentru capacitate de stocare adițională. Echipamentul dispune de 40 de porturi FC 32 Gbps echipate cu transceivere SFP și 40 de porturi 10 Gbps Ethernet echipate cu transceivere SFP. Porturile sunt distribuite în mod egal pe fiecare dintre controllerele echipamentului de stocare. În configurația existentă, echipamentul asigură o performanță de 900 IOPS per TB util prezentabil către host-uri cu deduplicare inline și compresie inline activate pentru workload de tip 70% acces random, 30% acces secvențial, 50% Read, 50% Write cu IO-uri de dimensiune de 32KB. Echipamentul de stocare din CPD se replică asincron/sincron cu cel din CSD prin SRDF. Echipamentul de stocare existent permite update de software, firmware fără restartarea controllerelor și este scalabil la 16 controllere și 16 TiB memorie cache globală.

Ambele echipamente beneficiază de garanție până la sfârșitul anului 2024.

### Infrastructura rețelei SAN

Infrastructura rețelei SAN (Storage Area Network) utilizează standardul Fiber Channel. Fiecare Centru de date dispune de câte două switch-uri SAN CISCO MDS 9710 Multilayer Director, configurate în mod redundant, echipate după cum urmează:

1. Centrul Primar de Date:
   1. MDS9710 #1:
      1. 3 sloturi disponibile pentru linecard-uri;
      2. 6 surse de alimentare.
   2. MDS9710 #2:
      1. 5 sloturi disponibile pentru linecard-uri;
      2. 6 surse de alimentare.
2. Centrul Secundar de Date:
   1. MDS9710 #3:
      1. 4 sloturi disponibile pentru linecard-uri;
      2. 6 surse de alimentare.
   2. MDS9710 #4:
      1. 4 sloturi disponibile pentru linecard-uri;
      2. 6 surse de alimentare.

MDS9710 #1 și MDS9710 #3 nu beneficiază de garanție, iar MDS9710 #2 și MDS9710 #4 beneficiază de garanție până la sfârșitul anului 2024.

### Infrastructura de comunicații Ethernet

Nivelul de acces utilizat pentru interconectarea echipamentelor, este realizat cu echipamente Cisco Nexus conectate într-o topologie redundantă utilizând legături cu lățime de bandă de 10 Gbps. Echipamentele sunt de tipul Nexus 5548UP și Nexus 2232PP și suportă transceivere SFP+ cu următoarele caracteristici:

1. SFP Ethernet Fiber 1Gbps: Cisco SFP-GE-T;
2. SFP Ethernet Fiber 10Gbps: Cisco SFP-10G-SR.

Echipamentele Nexus 5548UP și Nexus 2232PP nu beneficiază de transceivere SFP+ disponibile.

### Soluția de administrare platforme informatice

Soluția existentă, care este produsă de către SolarWinds, include următoarele modulele:

1. 1245 – SolarWinds Network Performance Monitor SL500;
2. 3052 – SolarWinds NetFlow Traffic Analyzer Module for SolarWInds Network Performance Monitor SL500;
3. 4100 - SolarWinds Network Configuration Manager DL50;
4. 57001 – Log Analyzer LA25;
5. 1361 – Server & Application Monitor SAM25;
6. 2501 – SolarWinds Web Performance Monitor WPM10;
7. 14004 – SolarWinds Virtualization Manager VM112;
8. 29000 – SolarWinds Database Performance Analyzer;
9. 58001 – Server Configuration Monitor SCM25;
10. 8804 – SolarWinds Storage Resource Monitor SRM500.

Soluția beneficiază de suport până la sfârșitul anului 2024.

### Baze de date

Bazele de date din cadrul Sistemului informatic al MF sunt pe tehnologie Oracle.

Între bazele de date din cadrul Sistemului informatic al MF au loc diverse replicări de date și accesări ale datelor, prin intermediul produselor software de replicare, precum Oracle DataGuard, Quest SharePlex și prin accesări de tip dblink.

### Soluția hardware-software pentru efectuarea și restaurarea salvărilor de siguranță

#### Platforma pentru efectuarea și restaurarea salvărilor de siguranță

1. Centrul Primar de Date:
   1. 1 x DELL EMC Data Protection Suite format din:
      1. DELL EMC NetWorker;
      2. DELL EMC Cloudboost;
      3. DELL EMC Avamar;
      4. DELL EMC Data Protection Search;
      5. DELL EMC vRealize Data Protection Extension;
      6. DELL EMC RecoverPoint for Virtual Machines.
2. Centrul Secundar de Date:
   1. 1 x DELL EMC Data Protection Suite format din:
      1. DELL EMC NetWorker;
      2. DELL EMC Cloudboost;
      3. DELL EMC Avamar;
      4. DELL EMC Data Protection Search;
      5. DELL EMC vRealize Data Protection Extension;
      6. DELL EMC RecoverPoint for Virtual Machines.

#### Echipament pentru efectuarea salvărilor de siguranță pe disc

1. Centrul Primar de Date:
   1. 1 x DELL EMC PowerProtect DD9900 echipat cu:
      1. 960 TB utili pe discuri NL-SAS;
      2. 8 x 16 Gbps FC;
      3. 8 x 10 Gbps Ethernet SFP+;
      4. 4 x 10 Gbps Ethernet Base-T.
2. Centrul Secundar de Date:
   1. 1 x DELL EMC PowerProtect DD9900 echipat cu:
      1. 960 TB utili pe discuri NL-SAS;
      2. 8 x 16 Gbps FC;
      3. 8 x 10 Gbps Ethernet SFP+;
      4. 4 x 10 Gbps Ethernet Base-T.

#### Biblioteci de benzi

1. Centrul Primar de Date:
   1. 1 x DELL EMC ML3/ML3E Tape Library echipat cu:
      1. 6 x controller ML3 LTO8 FC-FH Tape Drive, fiecare echipat cu:
         1. 2 x porturi 8 Gbps FC;
         2. 40 de sloturi de benzi per drive, total de 240 sloturi de benzi per bibliotecă;
         3. scalabilitate la 40 drive-uri LTO-8;
         4. scalabilitate la 280 sloturi de benzi
2. Centrul Secundar de Date:
   1. 1 x DELL EMC ML3/ML3E Tape Library echipat cu:
      1. 6 x controller ML3 LTO8 FC-FH Tape Drive, fiecare echipat cu;
         1. 2 x porturi 8 Gbps FC;
         2. 40 de sloturi de benzi per drive, total de 240 sloturi de benzi per bibliotecă;
         3. scalabilitate la 40 drive-uri LTO-8;
         4. scalabilitate la 280 sloturi de benzi

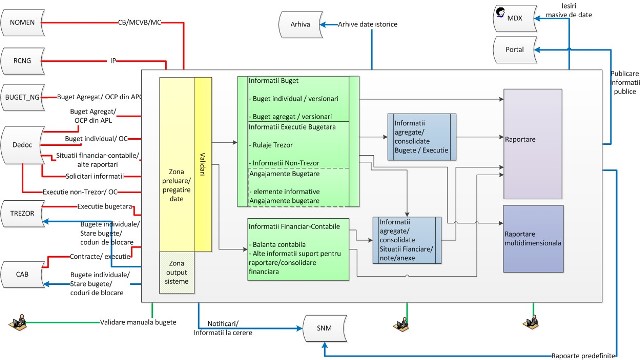
## Descriere mecanisme de integrare

### Forexebug

Sistemul informatic Forexebug cuprinde mai multe subsisteme care se interfațează cu aplicația Trezor la nivel central. Modalitatea de interfațare este prin replicare în timp real cu Shareplex, astfel:

1. CAB 🡺 Trezor – se transmit informații referitoare la angajamente și disponibil
2. Trezor 🡺 CAB – se transmit informații referitoare la operațiunile instituțiilor publice
3. Forexebug DW 🡺 Trezor – se transmit bugetele individuale ale instituțiilor publice
4. Trezor 🡺 Forexebug DW – se transmit rulajele zilnice aferente execuției bugetare
5. Nomenclatoare 🡺 Trezor – se transmit nomenclatoarele utilizate în Trezor
6. Registrul EP 🡺 Trezor – se transmite Registrul Entităților

Arhitectura sistemului



Tehnologie submodul Control Angajamente (CAB)



Tehnologie submodul Forexebug DW



#### CAB

Componentele de tehnologie utilizate sunt următoarele:

1. Baza de date CAB : Oracle Database SE 11.02.04
2. Server de aplicații: Oracle Weblogic Server SE 12.1.3
3. Java 6 (framework-uri principale folosite: Spring, Apache Wicket, iBatis)

#### Forexebug DW

Componentele de tehnologie utilizate sunt următoarele:

1. Baza de date ForExeBug DW : Oracle Database 11g Enterprise Edition
2. Oracle E-Business Suite 12.2.2 - Oracle General Ledger:
   1. Oracle Internet Application Server 10g (include Oracle HTTP Server)
   2. Oracle Forms Server 10g
   3. Oracle Reports Server 10g
3. Oracle Business Intelligence EE 11.1.1.7
   1. Oracle Database (schema pe ForExeBug DW)
   2. Oracle Weblogic Server
4. Essbase/ Hyperion
   1. Oracle Essbase Server (OLAP Server)
   2. Oracle Hyperion Planning
   3. Oracle Weblogic Server
   4. Oracle Database (schema pe ForExeBug DW)

#### Nomenclatoare și Registrul Entităților

Componentele de tehnologie utilizate sunt următoarele:

1. Baza de date – Oracle, versiune 11.2.0.3.0.
2. Java 6

#### ForexeSNM

Componentele de tehnologie utilizate sunt următoarele:

1. Baza de date - Oracle, versiune 11.2.0.1.0
2. Java 6

### SIAC

Aplicația SIAC folosește baze de date distribuite la nivelul unităților teritoriale de administrare fiscală – Oracle 8.0.5, Forms și Reports.

Modalitatea de interfațare între cele 2 aplicații este prin export/import de fișiere (.dmp) la nivel local:

1. Trezor 🡺 SIAC – zilnic – se transmit operațiunile efectuate pe conturile de taxe și impozite gestionate în SIAC și soldul unor conturi de disponibil, conform prevederilor legale;
2. SIAC 🡺 Trezor – zilnic – se transmit distribuiri, compensări, transferuri, restituiri, rambursări de TVA, etc..

### NOES

Aplicația NOES folosește baze de date distribuite la nivelul unităților teritoriale de administrare fiscală – Oracle 8.0.5, Forms și Reports.

Modalitatea de interfațare între cele 2 aplicații este prin export/import de fișiere (.dmp) la nivel local :

1. Trezor 🡺 NOES – zilnic – se transmit operațiunile efectuate pe conturile de taxe și impozite gestionate de NOES, conform prevederilor legale;
2. NOES 🡺 Trezor – zilnic – se transmit distribuiri, compensări, transferuri, restituiri.

### SAIVEN

Aplicația SAIVEN-GOTICA este o aplicație centralizată, folosește baza de date Oracle versiune Oracle 11.2.0.3.0. Tehnologia utilizată pentru aplicația GOTICA este: Oracle Application Server 10g (10.1.2.0.2). Configured Components: Oracle HTTP Server, Oracle Application Server 10g Containers for J2EE, Oracle Application Server 10g Web Cache, Oracle Application Server 10g Portal, Oracle Application Server 10g Forms Services, Oracle Application Server 10g Reports Services.

Modalitatea de interfațare între cele 2 aplicații se face la nivel local prin export de fișiere (.dmp) dinspre Trezor spre SAIVEN și prin export fișiere (.txt) dinspre SAIVEN spre Trezor:

1. Trezor 🡺 SAIVEN – zilnic – se transmit operațiunile efectuate pe conturile de taxe și impozite gestionate de SAIVEN
2. SAIVEN 🡺 Trezor – zilnic – se transmit distribuiri, compensări, restituiri (numerar, mandate poștale, virament), sponsorizări, etc..

### FTY-Star

Aplicația este la nivel central și foloseste baza de date Oracle 11g.

Modalitatea de interfațare cu aplicația Trezor se face printr-un serviciu WEB cu standard de formatare JSON, sincron.

### QpayIntegrator

Aplicația QPayIntegrator se interfațează cu aplicația Trezor prin intermediul conectorilor instalați pe serverul qPay și care se conectează la baza de date Trezor printr-o legătură securizată, de tip client - server utilizând un client de conectare Oracle.

### E-popriri

Aplicația TREZOR verifică existența popririi în sistemul Epopriri pentru plățile efectuate în contul unic de popriri deschis la trezoreria operativă centrală (funcție apelată prin DBLink).

Aplicația TREZOR pune la dispoziția sistemului Epopriri informații aferente plăților efectuate în contul unic de popriri deschis la trezoreria operativă centrală (operațiune efectuată prin DBLink).

# Cerințe generale ale soluției eTrezor

1. Soluția dezvoltată și implementată trebuie să fie flexibilă și să permită dezvoltarea unor funcționalități noi, în acord cu necesitățile și cerințele formulate de către Beneficiar și/sau în concordanță cu legislația în vigoare.
2. Se va asigura migrarea de date istorice pentru o perioada de minim 10 ani anterior intrării în producție a noului sistem informatic eTrezor, din aplicatiile Trezor, CashBNR, Cont Tranzitoriu, Dcredite, Dcredite\_BTS, Depterm, Emicert, Ibancls10g, etc., în funcție de concluziile activităților de analiză.
3. Fiecare componentă va fi dezvoltată împreuna cu documentaţia aferentă.
4. În urma dezvoltării și implementării sistemului eTrezor, Consultantul va pune la dispoziția MF toate livrabilele aferente soluției funcționale, incluzând descrierea tuturor componentelor, modulelor, nomenclatoarelor, manualele şi procedurile de operare şi instalare, precum şi orice produs rezultat (codul sursă, fişiere de configurare, scripturi de instalare, etc.).
5. Modelul operațional actual și modelul operațional tintă vor fi detaliate de către Consultant în cadrul activităților de analiză.
6. Sistemul eTrezor va fi integrat funcțional cu sistemele / componentele Forexebug, sistemele informatice ale ANAF pentru administrarea contribuabililor, DEDOC, FTY-Star, QpayIntegrator, E-popriri, managementul identității și alte sisteme / aplicații, în conformitate cu concluziile activităților de analiză. În acest scop, vor fi dezvoltate functionalitățile de integrare, schimb de date și interfețe cu acestea, precum și cu alte sisteme aflate în implementare sau în diferite stadii de dezvoltare care pot impacta sistemul eTrezor.
7. În funcție de concluziile activităților de analiză, în cadrul noului sistem informatic vor fi dezvoltate și integrate functionalitățile existente în aplicațiile actuale TREZOR, CashBNR, Cont Tranzitoriu, Dcredite, Dcredite\_BTS, Depterm, Emicert, Ibancls10g, Înrolare Forexebug, adaptate sistemului centralizat și cerințelor specifice cuprinse în prezentul document.
8. Funcționalitățile aplicațiilor și fluxurile prezentate la capitolul [5 Descrierea sistemelor informatice existente](#_Descrierea_sistemelor_informatice) sunt oferite cu titlu de exemplu, gama prestațiilor din contract nu va fi limitată strict la acestea.
9. Componentele sistemului eTrezor vor fi integrate.
10. La solicitarea Beneficiarului sau la propunerea Consultantului, în funcție de rezultatul activității de analiză:
    1. se vor automatiza proceduri / operațiuni / verificări, care în prezent se efectuează manual de către angajații UTTS / DGCP
    2. se vor optimiza / îmbunătăți procese.
11. Soluția ofertată trebuie:
    1. să fie elaborată în limba română
    2. să acopere toate cerinţele exprimate în Caietul de sarcini, care sunt cerințe minime şi obligatorii
    3. să detalieze modul de îndeplinire (de realizare) a tuturor cerințelor formulate în prezentul Caiet de sarcini
12. Soluția dezvoltată de către Consultant va asigura respectarea tuturor reglementărilor naționale în vigoare, a directivelor europene privind securitatea datelor, a tranzacțiilor, prelucrarea datelor cu caracter personal, protecţia datelor personale în cadrul activităţilor specifice desfăşurate de autorităţile de aplicare a legii, precum și serviciile de plată în cadrul pieței interne.
13. În cadrul ofertei sale, Consultantul va descrie modul în care soluția respectă prevederile Regulamentului UE 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date, Directiva (UE) 2016/680 referitoare la protecţia datelor personale în cadrul activităţilor specifice desfăşurate de autorităţile de aplicare a legii, precum şi Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne.
14. Pe întreaga perioadă de derulare a contractului, componentele sistemului eTrezor vor fi adaptate de către Consultant oricăror modificari ale cadrului legal și standardelor elaborate de organizaţiile abilitate, inclusiv în situația în care vor fi implementate alte sisteme specifice de plată care prezintă anumite particularităţi în comparaţie cu sistemele existente (de ex.: sistem de plată dedicat achitării amenzilor contravenţionale (în curs de implementare, în funcție de aprobarea prevederilor legale în domeniu)).
15. Funcționalitățile solicitate prin prezentul caiet de sarcini, componentele sistemului integrat la care acestea se referă, interconectarea și interacțiunea componentelor sistemului integrat eTrezor cu alte sisteme existente la nivelul MF și ANAF, scenariile de lucru posibile, criteriile de prioritizare privind procesarea, procedurile și cerințele de asigurare a continuității, vor fi elaborate, aprofundate, completate, dezvoltate și îmbunătățite de către Consultant în cadrul activităților de analiză, precum și pe întreaga perioadă de derulare a contractului.
16. În cazul în care se constată, în cadrul activităților de analiză, că nu mai sunt necesare anumite funcționalități din aplicațiile existente ca urmare a centralizării sistemului informatic, acestea nu se vor dezvolta.

## Cerințe funcționale ale soluției

1. Soluția dezvoltată și implementată de Consultant va integra utilizatori, informații, procese și perioade (pentru introducere, verificare, validare, transmitere electronică şi transfer date în/din eTrezor din/către alte sisteme). În acest sens:
   1. va fi dezvoltat și implementat un modul de administrare a sistemului eTrezor, accesibil administratorilor de aplicație și de sistem (grupuri distincte de utilizatori); funcționalitățile oferite de acest modul vor permite configurarea sistemului eTrezor și a componentelor acestuia, în conformitate cu concluziile activităților de analiză (de ex.: activarea / dezactivarea accesului la componentele eTrezor, a mecanismelor de autentificare dezvoltate, stabilirea orarului de funcționare, administrarea sistemului de mesagerie)
   2. accesul la functțonalitățile sistemului, pe componente, va fi posibil conform unui interval orar, stabilit prin regulile de sistem
   3. va fi implementat un modul de gestionare a utilizatorilor, prin intermediul căruia:
      1. se vor defini tipurile de utilizatori ai componentelor sistemului eTrezor și profilul asociat acestora; cu titlu de exemplu, se vor avea în vedere următoarele categorii de utilizatori ai sistemului eTrezor:
         1. utilizatori finali
            1. funcționarii de la nivelul UTTS și MF
            2. reprezentanții instituțiilor publice
            3. reprezentanții operatorilor economici
            4. persoane fizice
         2. utilizatori speciali (administratori de aplicație)
         3. personal de specialitate TIC (dezvoltatori, administratori de sistem)
      2. se vor putea defini grupuri de utilizatori (inclusiv clienți) și permisiuni acordate acestor grupuri (de exemplu: un utilizator înrolat în grupurile respective va beneficia de permisiunile acordate grupului)
      3. se vor gestiona permisiunile acordate utilizatorilor cu privire la interacțiunea cu sistemul integrat, componentele și modulele acestuia, conform drepturilor de acces acordate; în mod particular, pentru un utilizator care are acces în sistem, se vor putea acorda permisiuni de vizualizare a informațiilor aferente utilizatorilor specificați (unul, un grup sau toți), prin interacțiune cu componentele sistemului eTrezor
2. Vor fi dezvoltate și implementate funcționalități care sa permită clienților UTTS asigurarea posibilității derulării unor operațiuni prin intermediul oricărei UTTS, în conformitate cu concluziile activităților de analiză
3. sistemul și componentele dezvoltate trebuie să permită autentificarea utilizatorilor cu certificate digitale calificate, certificate digitale necalificate și / sau prin cont utilizator şi parolă – în funcție de tipul utilizatorilor (de ex.: în cazul utilizării sistemului cont utilizator/parolă - să prevadă obligativitatea schimbării parolei de acces la un anumit interval de timp configurabil și să permită resetarea acesteia în anumite situații); mecanismele de autentificare vor putea fi activate sau dezactivate, pentru fiecare componentă a sistemului eTrezor, prin intermediul modulului de administrare a sistemului informatic integrat;
4. va exista posibilitatea limitării numărului de încercari de logare sau de autentificare, iar accesul ulterior la sistem să fie permis de către un utilizator cu drepturi specifice sau cu posibilitatea reluării acțiunii de logare / autentificare după o perioadă de timp prestabilită
5. să ofere un mecanism prin care un utilizator să fie delogat în cazul în care nu a mai efectuat nicio tranzacţie/cerere de raportare într-o perioadă de timp (interval ce poate fi setat de administratorul sistemului). Componentele sistemului vor afișa timpul rămas până la deconectarea automată din aplicație (timp predefinit, setat de administratorul sistemului pentru fiecare componentă și tip de utilizator) și utilizatorul va fi informat că deconectarea automată va avea loc din motive de securitate
6. va fi implementat un modul de gestionare a conturilor gestionate de UTTS (ex: deschidere, blocare, deblocare, închidere, etc.)
7. va fi implementat un modul de gestionare a tranzacțiilor conform regulilor de business (ex: nu se pot efectua operațiuni între anumite conturi, se pot efectua operațiuni doar între anumite conturi)
8. va fi implementat un modul de gestionare a conturilor analitice (ex: deschidere, blocare, deblocare, închidere, etc.)
9. Soluția dezvoltată va fi funcțională și în situația în care structura contului IBAN utilizată în Sistemul Electronic de Plăți în România va fi modificată (de ex.: creșterea numărului de caractere a codului IBAN - de la 24 câte sunt în prezent). În acest sens, Consultantul va pune la dispoziția Beneficiarului documentația și instrumentele de implementare corespunzătoare.
10. va fi dezvoltat și implementat un modul privind gestionarea operațiunilor financiare, care va cuprinde informații precum, dar fără a se limita la:
    1. operațiunile care necesită validare (principiul celor 4 ochi)
    2. operațiunile care pot fi anulate ulterior validării (operațiuni care pot fi efectuate doar de anumiți utilizatori, cu un profil specific)
    3. regimul și cuantumul comisioanelor pe tipuri de operațiuni și actiuni ale utilizatorilor (de ex.: comisioane interbancare, comisioane aferente anulării unei operațiuni nedecontate și anulate ulterior validării, comisioane aferente plăților urgente, etc.)
11. va fi dezvoltată și implementată funcționalitatea de trasabilitate a tranzacțiilor efectuate și a stării acestora de către utilizatorii sistemului (de ex.: în derulare, nedecontat, autorizat, refuzat autorizare, returnat, anulat, finalizat). Stările vor putea fi însoțite și de o descriere sumară a motivului care le-a determinat (descrierea motivului putând fi modificată ulterior de anumiți utilizatori interni ai sistemului cu condiția afișării/stocării informației privind identitatea persoanei care a realizat respectiva modificare)
12. va fi dezvoltată și implementată funcționalitatea de anulare a unor documente (de ex: OPT, NC, chitanță, etc.) confirmate / autorizate și nedecontate / netransmise la organele fiscale
13. va fi dezvoltată și implementată funcționalitatea de decontare / autorizare a documentelor în funcție de prioritatea / tipul acestora (de ex.: decontarea / autorizarea plăților în regim de urgență, etc.)
14. vor fi dezvoltate funcționalități de a gestiona operațiuni în alte monede decat LEI (de exemplu; în EURO, în contextul aderării României la zona EURO)
15. va fi dezvoltată și implementată funcționalitatea de schimb de date în relația cu clienții (utilizatori finali - operatori economici sau instituții publice), atât prin mecanisme de comunicare masina-masina (servicii web), cât și prin import/export de fișiere
16. va fi dezvoltat un modul prin care să se poată gestiona validările care se efectueaza la înregistrarea în contabilitate a operațiunilor (de exemplu: activare / dezactivare validare), fără a fi necesară modificarea codului sursa
17. vor fi dezvoltate noi proceduri de validare, în funcție de rezultatul activităților de analiză (de exemplu: validări în cadrul operațiunilor de plată, între contul plătitor și beneficiar)
18. va fi dezvoltată și implementată funcționalitatea de programare (anunțuri) la unitățile Trezoreriei Statului pentru ridicare de numerar (inclusiv anulare);
19. comisioanele vor fi afișate pe ecran înainte de procesarea operațiunilor (de ex.: în cazul componentei Internet Banking)
20. va fi dezvoltată și implementată funcționalitatea de păstrare, accesare (vizualizare) și descărcare a istoricului operațiunilor efectuate (de ex.: ordinele de plată inițiate de către clienți și extrasele de cont vor fi disponibile utilizatorilor pe o perioadă configurată de către administratorii de sistem; perioada va putea fi configurată distinct pentru fiecare componentă a sistemului eTrezor)
21. va fi implementat un modul de management al documentelor, pe întregul ciclu de viaţă al acestora, care va permite încărcarea, gestionarea, urmărirea și stocarea documentelor în format electronic;
22. sistemul va respecta *Principiul proprietății asupra datelor* - numai proprietarul unei informaţii are dreptul să modifice sau să şteargă această informaţie. Proprietarul informaţiei este întotdeauna cel care a creat-o (a introdus-o în sistem). În concluzie, orice informaţie va avea un proprietar pe linie operaţională, la nivelul autorităţii proprietare, care va avea obligaţia să verifice corectitudinea informaţiei şi care va fi responsabil de orice modificare sau ştergere a acestei informaţii
23. sistemul va include un mecanism de jurnalizare (audit trail) a tuturor activităţilor întreprinse în sistemul eTrezor
    1. jurnalele trebuie să permită identificarea acţiunilor întreprinse în timp, precum:
       1. acţiunile de login (acces) în sistem (reușite sau nereușite)
       2. adăugarea, modificarea, ștergerea, anularea, confirmarea, transmiterea unei înregistrări eTrezor (documente, înregistrări contabile, înregistrări în nomenclatoare, etc.)
       3. interogarile și răspunsurile la interogări (inclusiv nereturnarea vreunui rezultat)
       4. informațiile introduse în sistem și recepționate de la sistem
       5. editarea de rapoarte din aplicația eTrezor
    2. jurnalele trebuie să permită identificarea utilizatorului care a executat respectivele acţiuni (nume utilizator, data şi ora accesării, adresa IP a echipamentului de la care a fost formulată cererea/executată operațiunea, componentele / modulele eTrezor accesate, tipul operațiunii realizate, etc.)
    3. datele din jurnale nu trebuie să poată fi modificate şi nu vor putea fi şterse înaintea termenului stabilit de păstrare
    4. acţiunile jurnalizabile vor fi activate, dezactivate și configurate prin modul de administrare a sistemului eTrezor
24. sistemul va include un mecanism de căutare a documentelor, rapoartelor, informaţiilor, după anumite criterii, cu prezentarea rezultatelor în conformitate cu drepturile și rolurile utilizatorului
25. sistemul va include un mecanism de export tranzacții / operațiuni contabile
26. sistemul va asigura confidenţialitatea, securitatea, integritatea şi disponibilitatea datelor tranzacţionate, procesate şi stocate, cel puțin prin:
    1. prevenirea accesului neautorizat în componentele / modulele eTrezor
    2. prevenirea modificărilor, distrugerilor neautorizate ale informaţiilor/datelor
27. va fi dezvoltată și implementată funcționalitatea de definire și gestionare sabloane – atât la nivel central, cât și la nivel operativ – cu ajutorul cărora se vor putea efectua mai rapid anumite operațiuni de plăți. Șabloanele vor fi putea fi utilizate în toate componentele / modulele sistemului, sau doar în anumite componente / module, după caz. Pentru platformele online, va exista posibilitatea de realizare a unor șabloane personalizate.
28. va fi proiectat, dezvoltat, implementat și testat un modul de analiză tranzacții și raportare, în conformitate cu concluziile activităților de analiză, care va cuprinde cel puțin următoarele:
    1. implementarea unui modul de analiză a tranzacţiilor, în scopul prevenirii, detectării și semnalării intențiilor de fraudă, precum și tranzacțiilor multiplicate; modulul livrat va conține mecanisme de analiză consacrate prin utilizare în cadrul instituțiilor de credit; de asemenea, modulul va putea fi extins de către Beneficiar cu alte mecanisme de analiză
    2. oferirea unor funcționalități de alerte (în scopul integrarii cu sistemul de monitorizare) și contramăsuri (de ex.: trecerea operațiunii într-o coada de investigare) la detectarea de suspiciuni de fraudă a tranzacţiilor efectuate, inclusiv mecanisme de raportare a acestora
29. va fi dezvoltat și implementat un modul unic de monitorizare pentru sistemul integrat eTrezor, componentele și modulele aferente; acest modul de monitorizare va îndeplini cel puțin următoarele funcționalități:
    1. va urmări diferiți parametri de funcționare, definiti în perioada de analiză (de ex.: sesiuni de conectare, IP, tip browser, rezoluție ecran, durată conexiune)
    2. monitorizare pe categorii de utilizatori și conturi
    3. funcționalități de raportare, pe diverse ierarhii organizaționale și componente eTrezor, în conformitate cu permisiunile utilizatorilor care le solicită (de ex.: o trezorerie să aibă acces la informațiile de monitorizare pentru clienții / beneficiarii arondați la respectiva trezorerie), cu posibilitatea de descărcare în diferite formate și de listare; cu titlu de exemplu, rapoartele vor furniza informații despre:
       1. operațiuni efectuate (de exemplu: starea în care se află operațiunile efectuate)
       2. situație clienți
       3. situatie conturi
       4. indisponibilitatea platformelor on-line (perioada de indisponibilitate pe zi/săptămână/lună/an);
    4. integrare cu modulul de analiză și raportare tranzacții
    5. afişare de statistici de utilizare a sistemului
30. va fi dezvoltat și implementat un modul de mesagerie pentru sistemul integrat eTrezor, cu componentele și modulele aferente
    1. acest modul de mesagerie va putea integra conținut de tip text, imagini
    2. modulul va permite evidențierea mesajelor necitite
    3. minimal, acest modul va gestiona mesaje, notificari și alerte, prin e-mail / interfață, în scopul aplicării acestora la evenimentele din viaţa sistemului
    4. prin interfața de administrare a acestui modul, mesajele transmise vor putea fi interpuse în diferite locuri (configurabile) în cadrul sistemului eTrezor
    5. pentru utilizatorii autentificați în sistem, modulul de mesagerie va susține activitatea de HelpDesk;
31. sistemul va include o secţiune de posibile întrebări privind utilizarea funcționalităților modulelor eTrezor, cu posibilitatea de a căuta după cuvinte cheie (help contextual)
32. va fi dezvoltată și implementată funcționalitatea de înregistrare automată în contabilitate a mesajelor de debitare / creditare directa în relația cu BNR (MT900, MT910), precum și posibilitatea de direcționare automată / manuală a acestor sume către conturile de disponibilități / bugetare aferente
33. Informațiile introduse de către utilizator vor fi validate, cu informațiile existente în sistem sau cu cifrele de control existente în cadrul elementelor (CNP, IBAN, CUI)

## Cerințe aplicabile platformei on-line

Platforma on-line pusă la dispoziția utilizatorilor va conține, minimal, o secțiune de termeni și condiții de utilizare a acestora, care va cuprinde (cu titlu de exemplu) informații privind legislația aplicabilă, cerințe privind controlul credențialelor şi măsuri pentru a preveni pierderea, dezvăluirea sau utilizarea neautorizată a acestora. Totodată, platforma on-line va cuprinde și o secțiune cu resurse (ex: legislație, formulare, ghiduri și manuale de utilizare) și link-uri utile.

Pentru a asigura omogenitate în interacțiunea cu platforma on-line dezvoltată, Consultantul va propune și implementa elemente comune de identitate vizuală pentru aceasta.

## Cerințe privind modulul de raportare și analiză

1. să permită acces la funcționalități, pe bază de roluri, utilizatorilor autentificați
2. să genereze rapoarte, inclusiv pe baza unor date istorice, conform unui nomenclator de rapoarte
3. să permită transmiterea de notificări prin email, aferente rapoartelor generate, către beneficiarii acestora, cu posibilitatea de a activa/dezactiva transmiterea
4. să existe posibilitatea de a prioritiza generarea de rapoarte
5. gradul de încărcare al modulului de raportare nu va avea un impact asupra performanței celorlalte componente ale sistemului eTrezor
6. are capacitatea de a rula rapoarte predefinite sau rapoarte ad-hoc
7. are capacitatea de a rula rapoarte pe baza unor solicitări inițiate din celelalte componente eTrezor
8. are capacitatea de a rula rapoarte predefinite la momente predefinite de utilizatorii cu rol de administrator
9. Soluţia ofertată trebuie să includă un modul de raportare şi analiză integrată (BI), care să ofere posibilităţi de modelare şi raportare intuitive prin intermediul unei interfeţe de tip Web. Acest modul va pune la dispoziție instrumente de analiză care să raspundă nevoilor operative sau de decizie din cadrul Trezoreriei Statului / MF.
10. Accesarea și administrarea modulului de raportare se va face prin intermediul unui browser fără a fi nevoie de instalarea de software-uri adiţionale. Accesul la date va fi personalizat în funcţie de drepturile şi rolurile persoanei care accesează modulul.
11. Modulul de raportare și analiză va îndeplini următoarele cerințe minimale:
    1. soluția trebuie să ofere rapoarte predefinite, pe bază de template-uri, precum şi posibilitatea de a genera rapoarte noi, ad-hoc, fără a fi nevoie de cunoştinţe de programare
    2. soluția ofertată trebuie să permită trecerea rapoartelor ad-hoc în rapoarte predefinite, fără a fi nevoie să fie reconstruite rapoartele
    3. solutia trebuie să permită generarea, distribuirea şi exportul rapoartelor în format PDF, Excel, CSV, XML, HTML, etc.
    4. să permită generarea de grafice de tip chart-uri, hărţi (inclusiv colorarea regiunilor, similar folosirii unui grafic de tip Pie)
    5. să ofere posiblitatea de drill-up, drill-down
    6. să pună la dispoziţie un sistem de auditare a accesului şi a activităţii la nivelul sistemului de raportare
    7. să permită definirea de grupuri de utilizatori şi roluri si să permită administrarea utilizatorilor care au acces în sistemul de raportare
    8. să permită salvarea rapoartelor şi vizualizarea unui istoric al rulării raportului
    9. să permită configurarea grafică a criteriilor de interogare <group by> , <order by>, <having>, etc.
    10. modulul de raportare trebuie să permită planificarea rulării rapoartelor şi trimiterea acestora către anumiţi utilizatori prin email sau salvarea într-o locaţie definită
    11. soluția ofertată trebuie să permită generarea de rapoarte pe baza informaţiei de accesare şi utilizare a sistemului de raportare
    12. soluția ofertată trebuie să permită generarea automată a cererii (query-ului), prin drag and drop al componentelor, fără a fi nevoie să fie creată în prealabil şi conectarea mai multor componente de prezentare la acelaşi query;
    13. soluția ofertată trebuie să permită rularea de rapoarte complexe (consumatoare de resurse / timp), prin care să se lanseze cerințe de generare asincrona a rapoartelor

## Cerințe modul de management al documentelor

Modulul de management de documente al sistemului eTrezor (DMS) va servi ca unic depozitar al documentelor și informațiilor din sistemul eTrezor. DMS va funcționa ca un instrument integrat de captură, administrare și înregistrare a conținutului și va gestiona cel puțin următoarele fluxuri:

1. Fluxuri operaţionale ce implică înrolarea utilizatorilor
2. Fluxuri operaţionale la ghişeu ce implică deschiderea/închiderea de cont:
   1. Captura și înregistrarea electronică a tuturor documentelor necesare procesului de deschidere/închidere de cont
   2. Captura specimenelor de semnătură şi a datelor din documentele de identitate ale clienţilor şi stocarea acestora;
   3. recunoaşterea automată a anumitor câmpuri din documentele de specimene de semnătură (obligatoriu CNP) şi documentele de identitate (obligatoriu CNP, seria şi numărul, perioada de valabilitate şi eventual, adresa) şi transformarea acestora în metadate care să poată fi transmise / verificate în eTrezor;
   4. interfaţarea şi integrarea operaţională la nivel de flux de date eTrezor, în conformitate cu concluziile activităților de analiză;
   5. vizualizarea de către operatori a conținutului încarcat în DMS, din modulele sistemului informatic eTrezor, în conformitate cu concluziile activităților de analiză.
3. Gestionarea fluxului operaţional pentru popriri - va fi aplicat pentru acele documente sosite numai în format letric şi implică:
   1. captura/scanarea adreselor de înființare a popririi și documentelor anexate care, în general, nu au o formă fixă sau standardizată şi stocarea acestora în DMS;
   2. recunoaşterea automată a anumitor câmpuri (cum ar fi: CUI / CNP, suma, IBAN, etc.) din documentele scanate şi transformarea acestora în date structurate și transferul lor automat către modulul de gestionare a popririlor din eTrezor;
   3. vizualizarea documentelor sursă pentru popriri încarcate în DMS de către operatori din modulele sistemului informatic eTrezor, în conformitate cu concluziile activităților de analiză.
4. Gestionarea fluxului operațional de preluare și înregistrare electronică a documentelor necesare inițierii unei tranzacții în sistemul eTrezor, depuse fie la ghișeu în format hârtie sau pe suport magnetic, fie încarcate prin portal, în conformitate cu concluziile activităților de analiză.

Minimal, în funcție de permisiunile atribuite, DMS va oferi utilizatorilor, în conformitate cu concluziile activităților de analiză, funcționalități de:

1. consultare a documentelor direct din componentele / modulele eTrezor pentru cei 5000 de utilizatori interni
2. înregistrare (depunere electronica) și stocare documente
3. captura prin scanare pentru fiecare dintre sediile MF/UTTS
4. gestionarea (manuală și automată) de atribute de tip metadate aferente documentelor încărcate
5. posibilitatea completării automate/manuale a unui termen de valabilitate a datelor/documentelor și transmitere alerte la expirarea valabilității datelor/documentelor
6. înregistrare și versionare documente
7. consultare (vizualizare) documente
8. căutare documente, în functie de anumite criterii (inclusiv metadate)
9. validare documente, conform unor reguli de business
10. generare de documente pornind de la șabloane predefinite
11. generarea și recunoașterea automată a codurilor de bare pe/de pe documente
12. aplicarea de semnături digitale și gestionarea documentelor semnate electronic
13. funcții de raportare a volumetriei de documente sau a eficienței unui proces derulat prin sistem
14. distribuire documente
15. securitatea privind accesul la documente
16. fluxuri de lucru (workflow) cu documentele înregistrate în sistem; se vor putea stabili reguli care vor dicta circulația documentelor în cadrul organizației, coroborat cu un mecanism de aprobare / avizare a acestora pe circuit

Modulul de management al documentelor va permite, în conformitate cu concluziile activităților de analiză, lucrul cu o gamă largă de tipuri de documente:

1. documente scanate (de ex., dar fără a se limita la GIF, JPEG, PNG, BMP, TIF, PDF)
2. documente semnate electronic cu certificat digital (inclusiv posibilitatea de verificare a semnăturilor digitale aferente acestor documente)
3. documente de tip container, semnate electronic cu certificat digital, cu atașamente, care pot fi procesate și încărcate în eTrezor (de ex. fișiere PDF cu XML atașat).

Prin modulul de management al documentelor se vor gestiona și specimenele de semnătură și documentele de identitate. Specimenele de semnătura și documentele de identitate vor fi preluate în sistem prin scanare sau transmitere online. Vor exista minim 400 de puncte repartizate în locațiile UTTS în care se vor putea prelua aceste date. Informațiile respective vor fi păstrate atât ca date, cât și ca imagine. Sistemul va transmite alerte cand aceste date au expirat.

## Cerințe soluție de înrolare a utilizatorilor

1. Să permită inițierea în mediul online a fluxurilor de înrolare în sistemele eTrezor și Forexebug
2. Să permită preluarea utilizatorilor deja înrolati în sistemul Forexebug
3. Să permită integrarea în solutie a elementelor grafice și de design specifice Ministerului Finanțelor / Trezoreriei Statului
4. Soluția trebuie să permita integrarea/automatizarea prin interfețe bazate pe tehnologii moderne, cu aplicații interne și externe. Minimal, tehnologiile digitale disponibile sau integrate nativ în sistem sunt: semnătura electronică, captura de date / OCR, automatizare documente, integrare cu sistemele MF (în conformitate cu concluziile activităților de analiză)
5. Interfețele / Fluxurile să fie customizabile ușor de către angajații MF, ulterior implementării / customizării inițiale
6. Soluția trebuie să permită definirea proceselor prin instrumente vizuale
7. Soluția trebuie să permită încărcarea documentelor necesare (incluzand, dar fără a se rezuma la BI/CI/pașaport, documente juridice ale entităților publice/private și ale reprezentanților acestora)
8. Să permită gestionarea datelor (informațiilor), documentelor și proceselor aferente fluxurilor de lucru specifice activității de trezorerie.
9. Fluxurile de lucru vor cuprinde urmatoarele etape principale, în conformitate cu concluziile activității de analiză, dar fără a se limita la acestea:
   1. Solicitarea de acordare/revocare roluri
   2. Prezentarea pașilor de urmat de către client
   3. Prezentare condiții de deschidere a relației cu Trezoreria Statului
   4. Completare informații personale, cum ar fi: număr de telefon mobil, adresa de domiciliu, adresa de corespondență (dacă diferă), adresa de e-mail, etc.
   5. Acceptare condiții de utilizare a datelor cu caracter personal
   6. Încărcare BI/CI/pașaport și validare, cât și alte documente, după caz, OCR date și stocare în DMS
   7. Selectarea modului de realizare a verificărilor (online, într-o unitate teritorială a trezoreriei statului)
   8. Acordarea/revocarea rolurilor solicitate
   9. Generarea documentelor și remiterea acestora pe e-mail
10. Să permită inițierea fluxului de înrolare specific de pe portalul aferent sistemului eTrezor, urmând ca procesul să poata fi continuat/definitivat, în funcție de opțiunea clientului
11. Să asigure posibilitatea primirii și capturării consimțământului online al clientului prin diferite forme
12. Să permită gestionarea regulilor de business
13. Motorul de reguli de business trebuie să fie suficient de flexibil și parametrizabil, astfel incât să poată fi configurat cu ușurință de către personalul MF/UTTS cu abilități tehnice și de business
14. Utilizatorii interni ai MF/UTTS trebuie să aibă acces la instrumente vizuale pentru revizuirea/modificarea modelelor de date, fluxurilor pentru utilizatori, configurarea regulilor de business (fără a se limita la acestea), fără a depinde de suportul din partea furnizorului
15. Soluția trebuie să dețină instrumente de monitorizare a proceselor de înrolare și starea acestora prin milestone-uri, rapoarte și dashboard-uri vizuale
16. Să permită acceptarea sau refuzarea unei solicitări, pe baza regulilor de business definite și afișarea motivării deciziei
17. Să ofere utilizatorului mesaje de informare referitoare la neîncadrarea în regulile de intrare în relația cu Trezoreria Statului
18. Să permită transferul fluxului de activități către un utilizator cu drepturi corespunzatoare, în sensul accesării informațiilor procesate de un alt utilizator din aceeași categorie de drepturi
19. Să permită transferul fluxului de activități către alți utilizatori, în cazul indisponibilizării utilizatorului care inițial a gestionat relația cu clientul
20. Să se poată vizualiza / evalua în timp real pe diverse nivele de supervizare statusul întregii activități, de către utilizatorii cu drepturi corespunzatoare din MF/UTTS
21. Să se poată seta nivele de alarmare pentru situații în care anumiți clienți stau prea mult într-o anumită etapă
22. Să permită încărcarea / descărcarea diverselor șabloane în diferite formate, utilizate în introducerea datelor și prelucrării acestora
23. Să emita alerte către persoanele responsabile, în cazul în care platforma constată că lipsesc documente obligatorii într-o anumită etapă din evoluția procesului. Platforma să poată fi configurată astfel încât să nu permită trecerea la următoarea etapă de procesare în lipsa unor documente obligatorii. În procesul de înrolare, platforma să permită trecerea pe un flux de evaluare în care clientul poate să vada dacă este eligibil pentru înrolare și să aducă documentul obligatoriu, care momentan poate fi indisponibil
24. Să permita gestiunea unui nomenclator cu tipuri de documente necesare înrolarii, în funcție de tipul clientului (entitate publică, operator economic, persoană fizică, etc.); tipurile de documente să poată fi declarate ca obligatorii sau opționale
25. Să permită reluarea fluxului pentru captura de documente și upload-ul imaginii lor cu adaugarea acestora în platforma de DMS
26. Să permită selectarea de către client a unității teritoriale a trezoreriei statului la care acesta dorește continuarea fluxului și stabilirea datei întâlnirii cu personalul din unitatea teritorială aleasă
27. Să asigure mecanisme de recunoaștere a clientului solicitant de servicii prin preluarea de imagini, selfie-uri și apeluri video
28. Să asigure disponibilitate în regim 24x7
29. Să conțină un mecanism de versionare și să permită gestiunea diferitelor versiuni a aceluiași document cu respectarea următoarelor principii:
    1. numai o versiune este validă, celelalte fiind gestionate numai în scop de informare
    2. oricare din versiuni poate fi/poate deveni cea validă
30. Să permită gestionarea utilizatorilor interni implicați în procesul de înrolare
31. Să conțină instrumente de parametrizare puternice, astfel încât să permită configurarea cu usurință a interfețelor utilizator, șabloanelor, fluxurilor de lucru, regulilor de business, etc.
32. Oferta va fi însoțită de lista de rapoarte specifice și analize efectuate asupra datelor procesate, care să includă cel puțin următoarele:
    1. Situația solicitărilor înregistrate cu specificarea statusului acestora și a motivului, în cazul nefinalizării înrolării
    2. Rapoarte privind duratele rezultate din parcurgerea fluxului de înrolare
33. Rapoartele vor putea fi generate în diferite formate: PDF, HTML, XLS, pe diverse criterii necesare activității MF/UTTS
34. Să includă liste de verificare și opțiuni de gestionare a încărcarii și alocării sarcinilor pe personalul implicat în activitatea de înrolare
35. Să se interfațeze pe fluxul operațional cu DMS, în scopul gestionării imaginii documentelor de identitate și a altor documente, în conformitate cu concluziile activităților de analiză
36. Accesul utilizatorilor interni la funcționalitățile soluției de înrolare se va face prin atribuirea de profile de utilizator la care sunt atașate drepturi. Profilele utilizatorilor vor fi definite conform responsabilității acestora. Profilele de utilizator și drepturile vor fi accesibile utilizatorilor interni cu drept de administrare, prin intermediul unei interfețe de administrare, în scopul gestionării modificărilor de profile existente, definirii de profile/drepturi noi și a asocierii dintre acestea
37. Soluția trebuie să permită unor utilizatori cu drepturi specifice, monitorizarea activităților derulate de către ceilalți utilizatori, având acces la rapoarte specifice, fără însă a avea posibilitatea alterării/modificării datelor și a configurațiilor programelor

## Asigurarea continuității funcționării sistemului eTrezor

Consultantul va analiza și va face recomandări pentru soluția cea mai potrivită de asigurare a continuității operaționale a sistemului eTrezor, ținând cont de necesitatea obținerii celei mai reduse perioade de indisponibilitate pentru toate componentele / modulele acestuia.

Soluția propusă de Consultant va fi proiectată şi implementată în aşa fel încât să asigure continuitate la defectarea componentelor. Componentele eTrezor vor avea capacitatea de a funcționa independent unele de celelalte (indisponibilitatea unei componente nu va atrage indisponibilitatea sistemului în ansamblu).

Obiectivele avute în vedere pentru asigurarea continuităţii activităţii sistemelor dezvoltate au drept scop reluarea şi recuperarea funcţiilor critice, în aceeaşi zi de decontare, pentru a asigura, în toate scenariile vizate, finalizarea tuturor tranzacţiilor aflate în aşteptare la data de decontare previzionată.

Pentru fiecare componentă a sistemului eTrezor, soluția trebuie să prevadă proceduri pentru asigurarea continuităţii serviciului într-un număr de scenarii posibile, printre care menționăm (fără a ne limita la):

1. situații neprevăzute sau cazuri de catastrofă majoră (cutremure, inundaţii şi incendii, etc.)
2. sabotaj
3. atacuri de tip cibernetic
4. erori umane
5. greve
6. fraude interne / externe
7. distrugeri de infrastructură (de ex.: cabluri electrice sau de rețea distruse)
8. întreruperi în furnizarea de energie electrică

Procedurile menționate - care vor permite continuarea sau, după caz, reluarea activității - vor fi implementate în totalitate până la punerea în funcțiune a sistemului.

# Cerințe funcționale specifice

## Cerințe funcționale specifice core banking

1. va fi dezvoltat și integrat un modul de gestionare a adreselor de înființare a popririi pe conturi. Cu titlu de exemplu, funcționalitățile asigurate de acest modul vor fi:
   1. gestionarea adreselor de înființare a popririi pe conturi / titlurilor executorii
   2. extragerea automatizată a datelor cheie din documentele nestructurate de tip popriri
   3. posibilitatea actualizării datelor aferente (sistări, anulări, restrângeri sume, etc.)
   4. indisponibilizarea sumelor aferente executării silite
   5. deblocarea sumelor aferente executării silite
   6. debitarea unui cont de trezorerie în vederea colectării sumelor indisponibilizate
   7. preluarea automată / manuală în aplicație a informațiilor referitoare la poprire, în funcție de baza legală de înființare a popririi (CPF - cod de procedură fiscală, CPC - cod de procedură civilă)
2. va fi dezvoltat și integrat un modul de deschideri / repartizări / retrageri de credite bugetare, care va oferi inclusiv funcționalități de tip management al documentelor (vezi Dcredite, Dcredite\_BTS, etc.)
3. va fi dezvoltat și integrat un modul de constituire și gestionare a depozitelor la termen (vezi DEPTERM)
4. va fi dezvoltat și integrat un modul pentru administrarea certificatelor de trezorerie (vezi EMICERT, EMIRAP)
5. va fi dezvoltat și integrat un modul pentru administrarea operațiunilor de retragere / depunere numerar (vezi CASHBNR)
6. va fi dezvoltat și integrat un modul pentru decontarea sumelor încasate prin intermediul conturilor tranzitorii deschise la nivelul instituţiilor de credit cu care MF are încheiate convenții (vezi Cont Tranzitoriu)
7. va fi dezvoltat și integrat un modul pentru administrarea IBAN-urilor (vezi Ibancls10g)
8. vor fi dezvoltate funcționalități de creare automată a conturilor analitice
9. vor fi dezvoltate funcționalități de preluare monetar la operațiunile de numerar
10. se vor dezvolta funcționalități prin care se pot interoga și genera rapoarte referitoare la datele istorice migrate din aplicatiile vechi
11. vor fi dezvoltate și implementate funcționalități de optimizare a proceselor pentru confirmarea tranzacțiilor (de ex.: în funcție de gradul de încărcare al utilizatorilor)
12. prin intermediul modulului de mesagerie, utilizatorii componentei core banking (funcționari din cadrul UTTS și administratori) vor avea acces la funcționalități de chat și de transfer de fișiere (de ex.: în vederea raportării de bug-uri, cu capturi de ecran)

## Cerinte functionale specifice Internet banking

Componenta Internet Banking va oferi utilizatorilor, prin intermediul unei platforme online, accesibilă 24/7, cel puțin posibilitatea de vizualizare a soldurilor conturilor deschise la unitățile Trezoreriei Statului, precum și funcționalități de gestionare a operațiunilor aferente acestora, în conformitate cu concluziile activităților de analiză.

Această componentă va pune la dispoziția utilizatorilor, prin rolurile atribuite, cel puțin funcționalitățile precizate în secțiunile [6.1 Cerințe funcționale ale soluției](#_Cerințe_funcționale_ale) și [6.2 Cerințe aplicabile platformei on-line](#_Cerințe_aplicabile_platformei), precum și:

1. posibilitatea de setare a unor limite/plafoane valorice de tranzacționare pe conturile clienților, configurabile de către utilizatori interni cu roluri specifice.
2. atribuirea unui rol de administrare a utilizatorilor din cadrul structurii clienților (entități publice sau operatori economici), prin care se vor stabili limitele / plafoanele valorice de tranzacționare pentru utilizatorii din cadrul structurii respective și tipurile de operațiuni permise pentru fiecare utilizator
3. Implementarea de funcționalități de blocare / deblocare a accesului în sistem a unui utilizator de către un alt utilizator cu rol specific;
4. posibilitatea de editare (modificare) a instrucțiunilor de plată, anterior validării / autorizării
5. import de date (de exemplu: fișiere XML), în vederea efectuării de operațiuni
6. acces la informații privind executările silite și posibilitatea efectuării de plăți aferente acestora, în funcție de prevederile legale în vigoare
7. posibilitatea de gestionare a conturilor analitice (solicitare deschidere/închidere conturi, etc.)
8. posibilitatea constituirii/lichidării de depozite și acces la informații privind depozitele deținute
9. posibilitatea achiziționării/transferului/răscumpărării de titluri de stat și acces la informații privind titlurile de stat deținute
10. acces la informații privind debitele fiscale administrate de ANAF, în masura în care acestea sunt puse la dispoziția sistemului, precum și posibilitatea efectuării de plăți aferente acestora
11. dezvoltarea și implementarea următoarelor modalități de autorizare, în conformitate cu concluziile activităților de analiză:
    1. operațiunile de plată să fie introduse de un utilizator, iar autorizarea să fie efectuată automat
    2. operațiunile de plată sa fie introduse de un utilizator, iar autorizarea să fie efectuată de un alt utilizator cu rol specific (din cadrul UTTS sau din cadrul structurii clientului)
    3. operațiunile de plată să fie introduse de un utilizator, iar autorizarea să fie efectuată automat pentru plățile încadrate într-o limita de sumă (inclusiv zero) sau de către un alt utilizator cu rol specific, pentru sume care depășesc această limită. Limita de sumă va putea fi setată fie de către MF/UTTS în profilul clientului, fie de către utilizatorul cu rol de administrare a utilizatorilor din cadrul structurii clienților (mai puțin decât limita stabilită de MF)
12. va fi dezvoltată funcționalitatea de limită (plafon) valorică, atât la nivel de tranzacție individuală, cât și cumulat, la nivel de perioadă; limita va fi configurabilă; se va putea aplica unui utilizator final, cont, client sau orice combinații ale acestor criterii; limitele de sume aplicabile operațiunilor vor putea fi setate la un nivel predefinit, stabilit prin regulile de sistem, nivel care ulterior poate fi modificat:
    1. fie de către MF/UTTS în profilul clientului
    2. fie de către utilizatorul cu rol de administrare a utilizatorilor din cadrul structurii clienților (mai puțin decât limita stabilită de MF).
13. posibilitatea de a încărca documente în cadrul fluxurilor de operații în modulul de Internet Banking
14. Deschidere de incidente la cererea clientului (Helpdesk)
15. Transmiterea răspunsului de la Helpdesk in internet banking
16. Soluția trebuie să poată opera pe echipamente de tip telefon mobil, tableta, calculator personal, laptop, pe care ruleaza un browser acceptat (cel puțin Google Chrome, Firefox, Microsoft Edge, Safari, Opera). Versiunile de browsere acceptate trebuie să fie cel puțin ultimele versiuni de la data punerii în producție a soluției.
17. Modulul Internet Banking va fi accesibil din portalul oferit în cadrul soluției
18. Mesajele de plată vor fi validate pe tot circuitul de procesare, atât la introducere, cât și la autorizare. În situația în care există erori pe circuitul de procesare, acestea vor fi înregistrate și comunicate, către parțile implicate.
19. Pentru autorizarea tranzacțiilor, va fi implementat un mecanism de verificare / autentificare multifactorială (de ex.: de tip token, e-token, SMS, OTP, etc.), în conformitate cu concluziile activităților de analiză.
20. Soluția trebuie să ofere posibilitatea derulării unui set complet de operaţiuni: plăţi intertrezorerii și interbancare, transferuri, constituire/lichidare depozite, achiziționare/transfer/răscumpărare titluri de stat, etc., acoperind astfel necesităţile obişnuite în derularea relaţiei client - trezorerie.
21. Soluția trebuie să permită, în conformitate cu concluziile activităților de analiză, urmatoarele facilități, dar fără a se limita la acestea:
    1. consultarea soldurilor conturilor și detaliile operațiunilor efectuate pe acestea, cu posibilitatea generării de extrase de cont;
    2. obținerea de informații aferente conturilor deschise;
    3. căutarea unei operațiuni anume după criteriile pe care clientul le stabilește singur și sortarea acestora dupa diverse criterii parametrizabile de către client în cadrul raportului obținut;
    4. efectuarea viramentelor în funcție de regulile de business;
    5. oferirea unui istoric al operațiunilor efectuate
    6. oferirea unei liste a beneficiarilor;
    7. schimbarea on-line a parolei;
    8. familiarizarea cu funcționalitățile acestui serviciu prin intermediul unei variante demonstrative accesabilă de către clienți;
    9. posibilitatea de consultare a întrebărilor și răspunsurilor frecvente în acest domeniu;
    10. accesarea ghidului/instrucțiunilor de utilizare a serviciului care să descrie modalitatea de utilizare a soluției;
22. Soluția va conține mecanisme care să permită procesarea tranzacțiilor inițiate în perioada în care în componenta core-banking se rulează procese specifice de închidere zi/lună/an

## Cerințe functionale specifice solutiei de prezentare (portal)

1. Va fi implementată o secțiune publică a portalului, care nu necesită autentificare și o secțiune privată a portalului, la care vor avea acces utilizatorii înrolați.
2. Prin intermediul secțiunii private a portalului, utilizatorii autentificați vor putea accesa componentele sistemului informatic eTrezor și cele ale Sistemului Național de Raportare Forexebug, în funcție de rolurile acordate.
3. Secțiunea publică a portalului va conține o secțiune de termeni și condiții de utilizare a acestora, care va cuprinde (cu titlu de exemplu) informații privind legislația aplicabilă, cerințe privind controlul credențialelor şi măsuri pentru a preveni pierderea, dezvăluirea sau utilizarea neautorizată a acestora. Totodată, va cuprinde și o secțiune cu resurse (ex: informații utile, legislație, formulare, proceduri, ghiduri și manuale de utilizare) și link-uri utile.

# Cerințe instruire

1. Furnizorul va asigura instruirea unui număr de 100 de utilizatori de business, persoane cheie de la MF/UTTS, pe principiul "train the trainers"
2. Furnizorul va asigura instruirea corespunzătoare a unui numar de minim 3 utilizatori de business pe fiecare componentă, ca administratori de aplicație/sistem
3. Furnizorul va asigura instruirea corespunzătoare a personalului tehnic al beneficiarului (pentru un număr de minim de 20 utilizatori), pentru a dobândi cunoștințele necesare administrării componentelor sistemului, modificării de funcționalități și dezvoltării de funcționalități noi
4. În scopul instruirii, furnizorul va pune la dispoziție și un manual de operare în format electronic, interactiv, care să acopere principalele etape și procese aferente fluxului operațional, împreuna cu un plan de seminar care să poată fi urmat de formatorii MF/UTTS în procesul de pregătire a restului personalului implicat

# Schimbarea cerințelor

1. Revizuirea priorităţilor de realizare şi implementare, precum şi a influenţelor asupra graficului de realizare a proiectului vor fi stabilite de comun acord fără a influenţa termenul de finalizare şi bugetul aprobat.
2. Rectificarea implementării defectuoase de către Consultant a cerinţelor formulate de către Beneficiar în activitatile de analiză, nu poate fi considerată schimbare de cerinţe.
3. Consultantul va analiza și va propune spre aprobare Beneficiarului orice soluții de îmbunătățire a sistemului, fără modificarea termenului de finalizare şi a bugetului aprobat.
4. Totodată, acolo unde se vor găsi nerespectări ale standardelor impuse sau se vor depista erori în prelucrare care nu au fost depistate în etapa de testare de acceptanță, sau alte deficiențe, Consultantul care a executat sistemul va face remedierile necesare, fără ca acest lucru sa fie considerat schimbare de cerinţe si fără perceperea de costuri suplimentare.

# Cerințe tehnice ale soluției eTrezor

## Cerințe generale

1. Soluţia dezvoltată și implementată de către Consultant, inclusiv din punct de vedere al produselor licentiate, nu trebuie să fie limitată la un număr de utilizatori, beneficiari, volum de date, tranzactii, alte elemente care au legătură cu soluţia furnizată sau să genereze costuri suplimentare de suport şi mentenanţă obligatorii post-producţie, ulterior finalizării contractului, inclusiv a perioadei de garanție
2. Toate documentele şi informaţiile primite de la Beneficiar, precum şi rezultatele tuturor activităţilor din cadrul acestui contract (cum ar fi: cod sursă, cod obiect, biblioteci, librării, manuale, documente de analiză, arhitecturi de sisteme, adrese, etc., fără a se limita la acestea) reprezintă informaţii confidenţiale, iar Prestatorul va asigura respectarea confidenţialităţii lor.
3. Prestatorul şi personalul său au obligaţia de a respecta confidenţialitatea documentelor şi informaţiilor menţionate mai sus, pe toată perioada executării contractului, pe perioada oricărei prelungiri a acestuia şi după încetarea contractului. În acest sens, Prestatorul, precum şi toţi experţii implicaţi în activităţile contractului sunt obligaţi să semneze un Acord de Confidenţialitate cu Beneficiarul la data semnării contractului.
4. Rezultatul tuturor activităţilor din cadrul acestui contract (cum ar fi: cod sursă, cod obiect, biblioteci, librării etc., fără a se limita la acestea) rămân proprietatea Autorităţii Contractante care le va putea modifica fără a fi nevoie de acordul Prestatorului.
5. Toate documentele, rapoartele şi datele, inclusiv diagrame, desene, specificaţii, planuri, formule, baze de date, software (cod sursă, cod obiect, biblioteci, librării etc.) şi orice alte materiale obţinute, compilate sau realizate de către Prestator în cadrul contractului (chiar dacă sunt module sau pachete program deja construite în alte proiecte sau în cadrul unor pachete disponibile comercial), sunt în proprietatea /proprietatea intelectuala a Autorităţii Contractante, aceasta având dreptul să le utilizeze, modifice, transfere fără acceptul Prestatorului sau al unei terţe părţi. Prestatorul le va furniza Autorităţii Contractante, fără a păstra copii şi fără a le utiliza în alte scopuri care nu au legătura cu contractul fără acordul scris al Autorităţii Contractante.
6. În cadrul proiectului pot fi oferite produse COTS, dar licențele si serviciile adiționale acestor licențe vor fi oferite gratis către MF, cu un timp de folosință nelimitat şi nu vor avea alte limitări; ofertantul va efectua o descriere detaliată a produselor COTS.
7. Soluția va fi licențiată integral. Soluția trebuie să se bazeze pe licențe perpetue pentru toate produsele software incluse în soluție (nu se admit licențe temporare sau cu funcționalități limitate comparativ cu licențe fără restricții pentru aceleași produse).
8. Ofertantul va indica dependenţele dintre produsele oferite.
9. Prestatorul nu va publica articole sau informaţii legate de serviciile prestate, nu va face referire la acestea în cazul prestării altor servicii către terţi şi nu va divulga informaţiile obţinute de la Beneficiar, fără acordul scris al acestuia.
10. Orice rezultate sau drepturi legate de acestea, inclusiv drepturi de proprietate intelectuală sau industrială, obţinute în cadrul contractului, sunt proprietatea Autorităţii Contractante, care poate dispune de ele după cum consideră.
11. Prestatorul va desfasura activitățile proiectului în conformitate cu standardele şi cele mai bune practici actuale din domeniul IT, vizând:
    1. programarea (performanţa, uşurinţa depanării, înţelegerea facilă şi posibilitatea de a modifica sau de a reutiliza codul furnizat)
    2. proiectarea bazelor de date
    3. proiectarea sistemului de prelucrare a fluxului de informaţie
    4. depanarea facilă a oricărei probleme sau erori apărute în funcţionarea sistemului
    5. securitatea datelor şi fiabilitatea sistemelor informatice
12. Codul sursă va fi furnizat cu respectarea următoarelor bune practici și standarde:
    1. indentarea liniilor de program în conformitate cu secvenţialitatea modulelor de program, a funcţiilor, a procedurilor, a porţiunilor de declarări de variabile, a porţiunilor în care se execută comenzi de lucru cu bazele de date, etc.
    2. comentarea liniilor de program care nu sugerează prin însuşi conţinutul lor funcţionalitatea sau scopul dorit, pentru un programator care ar încerca modificarea sau depanarea codului.
    3. comentarea obligatorie, explicită şi detaliată, a fiecărui început de modul, funcţie, procedură, porţiune de declarare de variabile, porţiune în care se execută comenzi de lucru cu bazele de date, etc.. Comentariul va conţine detalii explicite despre parametrii de intrare, rezultatele aşteptate ale modulului, funcţiei, etc.
    4. se va ţine cont de posibilitatea reutilizării codului în alte dezvoltări viitoare. Astfel, codul utilizat va fi optimizat pentru rularea rapidă, fără erori, va evita posibilitatea apariţiei pe anumite porţiuni a fenomenului de serializare, etc.
    5. de-a lungul întregului cod sursă se vor implementa submodule de interceptare a erorilor şi a excepţiilor care vor realiza afişarea într-un mod explicit, "human readable", a cauzei care a generat eroarea sau excepţia. Posibilele excepţii care pot apărea din incompatibilitatea parametrilor cu valorile acceptate vor fi anticipate şi tratate, astfel încât utilizatorul final nu va interacţiona cu mesaje sistem de eroare sau cu crush-uri de aplicaţie şi pierderi de date introduse. Submodulele de interceptare şi tratare a erorilor şi excepţiilor vor fi, de asemenea, comentate în detaliu, într-un mod explicit.
13. Sursele vor fi însoţite de o documentaţie detaliată, în special componentele care nu rezida in mod explicit, în sistem, sub formă de fişiere (ex: comenzi de tip scheduler, setări de sistem, setări şi parametri de instalare pe server de aplicatie, etc.).
14. Sistemul de prelucrare a informaţiei, în mod exhaustiv, nu va conţine puncte de serializare, puncte de single failover, erori de logică a fluxului de date şi a prelucrării datelor, va fi construit folosindu-se elementele cele mai actuale de bune practici recomandate de documentaţiile şi manualele de bune practici ale produselor folosite.
15. Pe toată perioada desfășurării proiectului, Prestatorul va realiza un transfer continuu și activ de cunoștințe către echipele tehnice și funcționale ale Beneficiarului, pentru ca acestea să poata prelua operarea, mentenanța și să poata realiza dezvoltări ulterioare ale sistemului creat fără a depinde de serviciile Prestatorului.
16. Sistemul trebuie:
    1. Să se integreze cu [Soluția hardware-software pentru efectuarea și restaurarea salvărilor de siguranță](#_Solutia_hardware-software_pentru) și să extindă această soluție la nivelul necesităților sistemului eTrezor

sau

* 1. să furnizeze o nouă soluție hardware-software pentru efectuarea și restaurarea salvărilor de siguranță compatibilă cu tehnologiile descrise la capitolul 5.17 Descrierea situației actuale la nivelul beneficiarului

1. Sistemul trebuie să se integreze cu Arhiva electronică
2. Sistemul trebuie să se integreze cu [serviciul de management al identității și control acces TIM/TAM](#_Descrierea_serviciului_de)
3. Sistemul trebuie să fie sigur, fiabil, fără puncte unice de cădere. Se va folosi Centrul de Date Secundar (CSD) pentru asigurarea continuităţii în arhitectură de înaltă disponibilitate.
4. Va fi implementată o soluție de tip „Disaster Recovery”
5. Livrarea și instalarea echipamentelor se va face la sediile beneficiarului.
6. Furnizorul va asigura integrarea echipamentelor furnizate în sistemul informatic existent al Autorității Contractante.
7. Pentru toate componentele și funcționalitățile menționate explicit, ofertantul va prezenta, în mod obligatoriu, informațiile relevante detaliate, inclusiv cod/model, fabricant, specificații detaliate de produs de la producător, cu indicarea în clar a documentului public pe site-ul producătorului, care să permită identificarea produselor oferite și confirmarea respectării cerințelor. În caz de neconcordanță, specificațiile oficiale publicate de producătorul echipamentului (valabile la data ofertei, pentru produsele oferite) vor fi considerate ca referință, iar conținutul acestora va prima asupra detaliilor tehnice ale ofertei.
8. Oferta tehnică va conține în mod obligatoriu și informațiile relevante detaliate, inclusiv cod/model, fabricant, cantitate pentru toate accesoriile și licențele software de interconectare necesare bunei funcționări a echipamentelor și licențelor software ofertate ca un tot unitar în concordanță cu cerințele tehnice și specificațiile funcționale minimale obligatorii ale caietului de sarcini.
9. Echipamentele hardware ofertate trebuie să fie produse unitare preconfigurate, existente în lista de produse standard a producătorului însoțite de documentația și descrierea aferentă. În acest sens, ofertantul are obligația de a include în propunerea tehnică documentația și descrierea fiecărui echipament ofertat, astfel cum acestea sunt asumate de către producător.
10. Toate echipamentele hardware ofertate și care vor fi livrate trebuie să fie noi și fabricate cu maxim 6 luni anterior datei de livrare, să nu fie declarate EoS (End-Of-Sale) sau EoL (End-Of-Life) la data ofertei, să fie nefolosite și să îndeplinească toate cerințele și specificațiile tehnice solicitate prin prezentul caiet de sarcini. De asemenea, nu sunt acceptate echipamente catalogate de producător ca fiind refolosite („refurbished”).
11. Ofertele vor include informații și documente (în original sau copie) despre certificări de calitate și conformitate cu standardele relevante și cu normele și recomandările Uniunii Europene aplicabile (cel puțin în ceea ce privește securitatea și interoperabilitatea electrică și electrostatică, securitatea operatorului uman, emisiile sonore sau de radiații, ergonomia și fiabilitatea). Produsele oferite vor fi autorizate să poarte marca CE sau CS. Pentru calitatea echipamentelor ofertantul va remite documente valabile emise sau obținute de producător.
12. Toate echipamentele ofertate, livrate, instalate și puse în funcțiune de către furnizor vor respecta standardele europene/românești în vigoare referitoare la siguranța în exploatare, compatibilitatea electromagnetică, marcaj CE și mediul înconjurător.
13. Furnizorul va instala toate echipamentele în spațiile tehnice indicate de către achizitor. Furnizorul va asigura conectarea echipamentelor la rețeaua electrică obligatoriu în mod redundant, atât la sursa de alimentare neîntreruptibilă (UPS) prin PDU-ul de rack dedicat (APC AP8853), cât și la rețeaua asistată de grupul electrogen prin cel de-al doilea PDU din rack dedicat (APC AP8853). Furnizorul va asigura pe cheltuiala sa toate materialele și accesoriile necesare conectării (de ex. cabluri electrice, siguranțe automate, cuple etc.)
14. Sistemele pe care vor rula solutiile software să fie de tip enterprise, dotate cu procesoare cu arhitectură pe 64 biti sau substantial echivalentă.
15. Sistemele de operare instalate pe serverele de aplicatii și baze de date să fie pe 64 de biti și să ofere suport nativ pentru cluster.
16. Sistemele de operare instalate pe serverele de aplicatii și baze de date să fie din familia Windows, UNIX şi distribuţii majore Linux și de tip enterprise.
17. Sistemul oferit să fie în configurație virtualizată.
18. Soluția trebuie să se integreze cu soluția existentă [F5 Networks](#_Descrierea_sistemului_de).
19. Soluția trebuie să se integreze cu platforma existentă de virtualizare VmWare.
20. Soluția trebuie să se integreze cu soluția existentă Microsoft Active Directory Forest level 2022 și orice suport hardware folosit să dispună de sistem de operare compatibil (Microsoft Server 2019 sau mai nou, Microsoft Windows 10 sau mai nou) și comunicarea LDAP respectă minim TLS1.3
21. Soluția trebuie să furnizeze un portal pentru utilizatorii interni
22. Soluția trebuie să furnizeze un portal pentru utilizatorii externi
23. Soluția va conține un modul integrat de elaborare fluxuri electronice (eFlows)
24. Soluția trebuie să fie scalabilă, astfel încât să poată fi adaugate ulterior resurse hardware suplimentare.
25. Arhitectura sistemului informatic integrat trebuie să îndeplinească un set de cerințe minimale:
    1. Să ofere scalabilitate
    2. Să ofere înaltă disponibilitate la fiecare nivel al sistemului informatic
    3. Să asigure securitatea tranzacțiilor desfașurate prin sistemul informatic
    4. Să asigure securitatea datelor, precum și posibilitatea de a recupera/corecta date din backup-uri
26. Soluția va conține:
    1. Un mediu de producție
    2. Un mediu de dezvoltare
    3. Un mediu de testare
    4. Un mediu de acceptanță
27. Până la finalizarea instalării și configurării mediilor de dezvoltare și testare la sediile Beneficiarului, Consultantul poate demara activitățiile de dezvoltare a sistemului informatic pe propriile echipamente
28. Soluția trebuie să fie cloud ready (soluția să poată rula într-un cloud)
29. Soluția să utilizeze o amprentă cât mai mică de procesare/memorie
30. Pentru toate echipamentele furnizate, garanţia hardware va fi de minim 36 de luni. Garanţia hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect şi înlocuirea acestuia în maxim 3 zile lucratoare, fără alte costuri.
31. Suportul software va fi de minim 36 de luni. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcţionare şi solicitarea rezolvării acestora în funcţie de severitate. De asemenea se va asigura dreptul de a face update-uri şi upgrade-uri la toate componentele software (sistem de operare, firmware, etc.)
32. Pe durata evaluării ofertelor, autoritatea contractantă are dreptul de a solicita ofertanților să pună la dispoziție echipamentele ofertate, pentru verificarea conformității între produs și ofertă. Orice neconformitate duce la descalificarea ofertei.

### Accesibilitate (Accessibility)

1. Sistemul trebuie să aibă doar interfață web cu utilizatorul, adică toate funcțiile pot fi accesate prin intermediul unui browser web și nu necesită instalarea pe stațiile de lucru client plug-in-uri sau add-on-uri sau similar.
2. Sistemul va livra conținut prin intermediul browserelor web populare, cum ar fi Microsoft Edge, Mozilla, Chrome, Safari, Opera, etc..

### Administrare (Service Management)

1. Sistemul trebuie să ofere capacitatea de a utiliza scripturi/instrumente automate pentru mascarea datelor pentru medii de testare, dezvoltare și acceptanta. Aceasta include scramblarea datelor și anonimizarea datelor.
2. Sistemul trebuie să ofere capacitatea de a utiliza scripturi/instrumente automate pentru subsetarea bazelor de date pentru a crea o versiune redusă a bazelor de date de producție pentru a fi utilizate în dezvoltare sau testare.
3. Furnizorul de soluții va asigura suport pentru toate mediile de dezvoltare, testare, acceptanță și de producție, segregate în mod clar și va oferi proceduri robuste pentru migrarea obiectelor în astfel de medii.

### Audit și Control (Audit and Control)

1. Sistemul va furniza jurnale de audit pentru tranzacții și detalii despre valorile câmpului înainte de modificare și valoarea câmpului după modificare.
2. Sistemul va avea capacitatea de a înregistra evenimente/acțiuni (completări, modificări, ștergeri date).
3. Sistemul va avea capacitatea de a înregistra evenimente/acțiuni legate de procesul de identificare și autentificare.
4. Sistemul va avea capacitatea de a înregistra acțiunile efectuate de personalul de asistență tehnică și de suport tehnic.
5. Sistemul va avea capacitatea de a înregistra acțiunile de urgență care sunt efectuate de personalul de asistență și securitate a sistemului.
6. Sistemul va oferi capacitatea de a înregistra atributele cheie ale evenimentelor auditate pe piste de audit, să includă, dar fără a se limita la data și ora evenimentului, ID-ul de utilizator al unei persoane care efectuează acțiunea, tipul evenimentului, activul sau numele resursei și tipul de acces, succes sau eșec al evenimentului.
7. Sistemul va avea capacitatea de a înregistra pistele de audit ale unui eveniment specific, cum ar fi o sursă (terminal, port, locație, adresă IP), unde este posibil din punct de vedere tehnic.
8. Sistemul trebuie să înregistreze fiecare încercare eșuată pentru accesarea / modificarea fișierelor de securitate, a tabelelor de parolă sau a dispozitivelor de securitate
9. Sistemul trebuie să ofere capacitatea de a capta, reține și analiza pistele de audit autorizate și neautorizate
10. Sistemul va avea capacitatea de a înregistra fiecare încercare eșuată de a accesa / modifica informațiile confidențiale și de a raporta în termen de 24 de ore.
11. Sistemul trebuie să furnizeze capacitatea de audit configurabilă cu controale de securitate definite de un utilizator cu drept de administrator.
12. Sistemul trebuie să ofere capacitatea de a audita tranzacțiile de configurare.
13. Sistemul furnizează auditul tuturor tranzacțiilor cu flux de lucru și semnături / aprobări electronice.
14. Sistemul trebuie să ofere capacitatea de a audita tranzacțiile de internet și intranet. Datele înregistrate includ, dar nu se limitează la adresa IP, data și ora și înregistrările de tranzacții istorice.
15. Furnizorul de soluții va dezvolta controale preventive și de detectare pentru a preveni sau limita riscul de erori neintenționate sau de utilizatori neautorizați care accesează sistemul sau modifica datele.
16. Furnizorul de soluții trebuie să furnizeze instrumente automatizate pentru a revizui sistemul și pistele de audit ale infrastructurii referitor la acțiunile utilizatorilor.

### Baze de date (Databases)

1. Sistemul trebuie să ofere capacitatea de compatibilitate în urma (backward compatibility) pentru datele arhivate.
2. Bazele de date reprezintă o componentă critică în cadrul infrastructurii, de aceea, pentru bazele de date se solicita un sistem dedicat care sa conțină toate componentele necesare (servere pentru bazele de date, soluție de stocare, infrastructura de comunicații) pentru a fi complet redundant, scalabil și capabil să ofere performanțe ridicate.
3. Sistemul de gestiune al bazelor de date relaționale trebuie să fie un sistem de administrare a bazelor de date de tip relațional care să fie disponibil comercial și să ofere posibilitatea de a rula pe diverse platforme hardware, precum și pe sistemele de operare majore existente pe piață (Windows, Linux, Unix). Nu se admit platforme bazate pe licențiere GPL sau produse customizate special pentru acest proiect. Caracteristicile existente ale produsului trebuie să fie regăsite în documente publice.
4. Accesul la informațiile stocate în baza de date trebuie să se efectueze în următoarele condiții:
   1. Datele să poată fi protejate împotriva defectării componentelor sistemului de baze de date;
   2. Funcționarea aplicației să nu fie afectată în cazul unor întreruperi planificate sau neplanificate ale unei componente din sistemul de baze de date;
5. Sistemul trebuie să cuprindă următoarele baze de date:
   1. Baze de date de producție, testare, dezvoltare, acceptanță pentru sistemul tranzacțional (OLTP)
   2. Baze de date de producție, testare, dezvoltare, acceptanță pentru sistemul de raportare (OLAP)
   3. Baze de date de producție pentru soluția de Disaster & Recovery, atât pentru sistemul tranzacțional (OLTP), cât și pentru sistemul de raportare (OLAP)
6. Componentele core-banking și Internet Banking vor avea baze de date distincte
7. În vederea reducerii furniturii hardware și a licențelor aferente, sistemul pentru baze de date trebuie să permită consolidarea de multiple baze de date (producție, test, dezvoltare și acceptanță).
8. Să permită administratorilor bazelor de date să poată specifica, ca anumite obiecte ale bazei de date să fie stocate permanent direct în memoria cache.
9. Posibilitatea ca scrierile în baza de date să se efectueze în memoriile cache.
10. Baza de date trebuie să permită funcționarea într-o arhitectura de disponibilitate înaltă de tip cluster activ-activ, o singură bază de date putând fi instalata pe mai multe noduri, asigurându-se toleranță la defecte hardware sau nefuncționare planificată. Această arhitectură pe lângă disponibilitate trebuie să ofere și:
    1. balansarea încărcării între noduri la nivelul cererilor și execuțiilor pe baza de date cluster, inclusiv posibilitatea de a interoga memoria cache de pe celelalte noduri, oferind o încărcare uniformă a acesteia, iar din punctul de vedere al utilizatorilor trebuie să ofere o disponibilitate de tip 24x7 în cazul apariției unei defecțiuni hardware la unul din serverele cluster-ului de bază de date;
    2. securitate tranzacțională:
       1. în cazul apariției unor erori hardware sau software în clusterul de bază de date trebuie să fie tratată de mecanismele interne ale bazei de date
       2. în cazul unei defecțiuni hardware și/sau software să permită reconectarea automată la nodul sau nodurile rămase disponibile;
    3. propriul software de clustering și management al discurilor, astfel încât să permită rularea pe diferite platforme, sisteme de operare sau sisteme de fișiere, fără achiziționarea de soft adițional de la producătorul sistemului de operare, asigurându-se totodată scalabilitatea orizontală a bazei de date și ușurință în administrare
11. Pentru asigurarea performanței maxime și asigurarea unui răspuns proactiv la eventualele degradări ale acesteia, baza de date trebuie să ofere:
    1. mecanisme interne de monitorizare și diagnosticare continuă, automatizând colectarea de parametri de funcţionare ai bazei de date, precum și stocarea acestora pentru a putea furniza o imagine pe termen lung a modului de funcţionare a bazei de date.
    2. automatizarea procesului de optimizare al instrucţiunilor SQL, explorând în mod cuprinzător toate modalitățile de optimizare ale unei instrucțiuni SQL (inclusiv recomandarea de a fi creați indecși sau partiții adiționale), oferind sugestii de implementatare pentru administratori și posibilitatea de implementare fără a fi necesară modificarea codului aplicației.
12. trebuie să asigure mecanisme robuste de criptare a datelor stocate, cât și a celor vehiculate în timpul sesiunilor dintre utilizatori și baza de date. Toate operațiile de criptare trebuie să poată fi implementate într-un mod transparent, fără a implica modificări la nivel de aplicație de business sau client. În funcție de nevoie, criptarea transparentă a datelor stocate trebuie să poată fi facută la nivel de coloană, tabelă sau chiar bază de date.

### Backup

1. Sistemul trebuie să ofere capacitatea de a utiliza o copie de rezervă pentru a restabili doar datele necesare în mediul existent, în cazul în care se pierd cantități mici de date din cauza ștergerii accidentale sau a coruperii de fișiere.
2. Sistemul trebuie să ofere capacitatea de a utiliza o copie de rezervă pentru a restabili un mediu alternativ în caz de dezastru care duce la deteriorarea sau indisponibilitatea datelor pe un întreg sistem.
3. Sistemul trebuie să ofere capacitatea de a efectua o copie de rezervă la rece completă a tuturor datelor (sistem de fișiere).
4. Sistemul trebuie să ofere capacitatea de a efectua copii complete „hot backup”.
5. Sistemul trebuie să ofere capacitatea de a efectua procese de salvare de date ( data backup ) în timpul ferestrelor de întreținere programate.
6. Sistemul trebuie să ofere capacitatea de a efectua procese de salvare a datelor cu sistem de verificare / recuperare a erorilor încorporat.
7. Furnizorul de soluții va propune proceduri și standarde pentru a implementa o politică și o strategie convenită de salvare a datelor, care include metoda (de exemplu, completă sau diferențială/incrementală), frecvență, stocare în afara locatiei, testare, protecție fizică și de mediu, restaurare și criptare.
8. Furnizorul de soluții va propune proceduri și standarde pentru implementarea politicilor de retentie a datelor, standarde, reguli legale și de afaceri, aprobate de Ministerul Finanțelor.
9. Soluția trebuie să suporte extracția și importul de date cu volume mari (prin aplicație proprie și / sau ETL, încărcare de fișiere).
10. Posibilitatea de a crea un export complet de date (pentru migrări viitoare/ulterioare).

### Colectare date (Data Entry)

1. Sistemul trebuie să ofere capacitatea de a permite validarea și editarea completă a datelor la introducerea lor/la punctul de intrare (on-line sau lot).
2. Sistemul trebuie să ofere capacitatea de a stabili reguli pentru fiecare tip de câmp/tranzacție care determină dacă datele/campurile sunt Necesare, Opționale sau Nepermise.
3. Sistemul trebuie să ofere capacitatea de a preveni postarea tranzacțiilor până când toate câmpurile „necesare” sunt completate și validate.
4. Sistemul trebuie să ofere capacitatea de a evidenția erorile de pe ecran în vederea unei corecții imediate (verificări online de validitate imediată).
5. Sistemul trebuie să ofere capacitatea de a valida volume/seturi de date introduse ca procesare batch, în conformitate/păstrând regulile de validare privind consistența datelor.
6. Sistemul va oferi capacitatea de a stabili reguli de validare obligatorii la nivel de sistem și reguli de validare suplimentare de sistem pentru volume/seturi de înregistrări.
7. Sistemul va furniza capacitatea de a reține/păstra tranzacțiile nevalide de la încărcarea unui volum de date într-un fișier de excluderi sau în tabele de eroare.
8. Sistemul trebuie să ofere capacitatea de a stoca preferințele utilizatorului pentru meniu, ecran, coloană și câmp, precum și pentru valorile implicite
9. Sistemul va oferi capacitatea de introducere a datelor pe baza profilurilor de securitate, în conformitate cu cerințele și controalele sistemului, care sa includă controale de acces bazate pe roluri.
10. Sistemul trebuie să ofere capacitatea de a valida logica de afaceri (verificări ale editarii) în mod automat pentru toate datele introduse.
11. Sistemul trebuie să ofere capacitatea de a permite semnături electronice pentru tranzacții.

### Disponibilitate (Availability)

1. Sistemul eTrezor trebuie să aibă o disponibilitate de cel puțin 99,5%.
2. Sistemul eTrezor va fi disponibil pentru a fi utilizat 24x7/365, cu excepția timpului de întreținere programată, fără toleranță suplimentară externă hardware/software (virtuală sau cluster).
3. Componentele sistemului OLTP trebuie să aibă cel puțin 99,5% disponibilitatea sistemului și continuitatea afacerii (adică recuperare în caz de dezastru, fail-over).
4. Componentele sistemului OLAP trebuie să aibă cel puțin 99,5% disponibilitatea sistemului și continuitatea afacerii (adică recuperare în caz de dezastru, fail-over).
5. Sistemul va oferi capacitatea de regăsire și gestionare a datelor într-un mod precis, fiabil și în timp util.
6. Sistemul va fi disponibil pentru a fi utilizat din locații externe rețelei deținute de Ministerul Finantelor, inclusiv VPN
7. Sistemul trebuie să furnizeze capacitatea de procesare a tranzacțiilor 24x7
8. Soluția trebuie să permită comutarea de la platforma de producție din CPD către platforma de producție din CSD în maxim 1 oră
9. Sistemul OLTP de producție din CPD va fi restabilit la nivel operațional în termen de 8 ore (după modificări specifice de configurare) din momentul în care apare un dezastru.
10. Sistemul OLTP de producție din CSD va fi restabilit la nivel operațional în termen de 48 de ore de la momentul în care apare un dezastru.
11. Sistemul OLAP de producție din CPD va fi restabilit la nivel operațional în termen de 8 ore (după modificări specifice de configurare) din momentul în care apare un dezastru.
12. Sistemul OLAP de producție din CSD va fi restabilit la nivel operațional în termen de 48 de ore de la momentul în care apare un dezastru.
13. Furnizorul de soluții trebuie să furnizeze metode de actualizare tehnică și de actualizare a aplicației fără întrerupere a disponibilității pentru utilizatorul final.

### Documentație (Documentation)

1. Furnizorul de soluții trebuie să furnizeze standarde și proceduri pentru formate, șabloane, structura fișierelor de documente și arhivă.
2. Furnizorul de soluții trebuie să furnizeze toată documentația, organizată în mod corespunzător pentru consecvență și ușurință de utilizare pentru a sprijini în mod eficient utilizatorii finali pentru:
   1. Utilizarea caracteristicilor și funcțiilor aplicațiilor;
   2. Adaptarea caracteristicilor aplicațiilor și fluxurilor de lucru pentru a se potrivi cu schimbarea din procesele de afaceri;
   3. Interfețele oferite către și dinspre alte aplicații;
   4. Personalizarea aplicațiilor furnizate de vendor;
   5. Operarea și monitorizarea proceselor de sistem și de aplicatie;
   6. Recuperare în caz de probleme de sistem, aplicație și date.
3. Furnizorul de soluții trebuie să furnizeze documentație ușor de utilizat, de înțeles și de accesat.
4. Furnizorul de soluții trebuie să furnizeze documentație pentru actualizările sistemului, remedieri de erori și patch-uri de întreținere.
5. Furnizorul de soluții furnizează întreținerea continuă a documentației, ori de câte ori este necesar
6. Furnizorul de soluții va transmite documentația și într-un format care poate fi modificat de Ministerul Finanțelor.
7. Furnizorul de soluții va furniza documentația pentru toate produsele, inclusiv, dar fără a se limita la instalare, administrare, dezvoltare, depanare , salvare, recuperare în caz de dezastru, etc..

### Fluxuri de lucru (Workflows)

1. Sistemul trebuie să ofere capacitatea de a utiliza fluxuri de lucru (workflows) pentru a direcționa electronic documentele asociate tranzacțiilor.
2. Sistemul oferă capacitatea inițiatorilor procesului de aprobare de a urmări procesul de aprobare.
3. Sistemul trebuie să ofere capacitatea ca pentru motorul fluxurilor de lucru (workflow engine) regulile să fie stabilite pe baza criteriilor definite de utilizator (atât pentru UI, cât și pentru API).
4. Sistemul va oferi capacitatea de a modifica atribuțiile fluxului de lucru la diferiți aprobatori autorizați pe baza disponibilității (atât din UI, cât și din API).
5. Sistemul va oferi capacitatea de notificări automate bazate pe reguli definite de utilizator, configurabile, inclusiv, dar fără a se limita la:
   1. Alerte de sistem (de exemplu, ferestre pop-up)
   2. Sistem de notificare
   3. Link-uri web
   4. Documente generate automat, gata de imprimare, formatabile (atât fișiere atașate imprimate, cât și e-mail)
6. Sistemul permite procesarea de aprobare secvențială sau concomitentă a tranzacțiilor, pe baza configurațiilor predefinite.
7. Sistemul permite delegarea aprobărilor (sau aprobări prin procură) pentru perioade de timp limitate sau nelimitate (de exemplu, vacanțe).
8. Sistemul furnizează reguli de escaladare automată pentru un workflow.
9. Sistemul permite utilizatorului să stabilească reguli de escaladare de la caz la caz pentru un workflow.
10. Sistemul va oferi capacitatea de a afișa aprobările anterioare și modificările unei tranzacții, iar lista va fi disponibilă tuturor utilizatorilor din rutarea fluxului de lucru pentru fiecare tranzacție și tip de tranzacție.
11. Sistemul va oferi capacitatea de a notifica prin e-mail, după cum este necesar, despre lucrări în așteptare, cum ar fi revizuirea și aprobarea pentru toate tranzacțiile care sunt dirijate prin fluxul de lucru electronic.
12. Sistemul trebuie să furnizeze un instrument de raportare și/sau interogare care poate raporta starea tranzacției care tranzitează prin fluxul de lucru.
13. Sistemul trebuie să ofere capacitatea de a personaliza și configura fluxul de lucru pentru rutarea și aprobarea acțiunilor pe baza tipului de tranzacție.

### Integrare (Integration)

1. Sistemul trebuie să ofere capacitatea de a fi interoperabil cu sistemele existente ale Ministerului Finanțelor, cu care este necesară interfațarea.
2. Sistemul trebuie să ofere capacitatea de a utiliza data pentru tranzacții, inclusiv suport pentru introducere cu data viitoare ( value date ) și procesarea automată a tranzacțiilor retroactive.
3. Sistemul trebuie să furnizeze setul de instrumente de integrare pentru proiectarea ecranelor utilizatorului final.
4. Sistemul trebuie să ofere capacitatea de a configura ecranul de conectare cu „branding” pentru Ministerul Finanțelor / Trezoreria Statului (logo, scheme de culori, precum și atentionări și mesaje pentru utilizatori).
5. Sistemul trebuie să ofere capacitatea de a atașa fișiere de diferite formate (inclusiv, dar fără a se limita la XML, PDF, Excel, Word) la fiecare tranzacție/înregistrare.
6. Sistemul trebuie să ofere capacitatea de a atașa fișiere la nivel de rând/înregistrare a diferitelor formate de fișiere (incluzând, dar fără a se limita la XML, PDF, Excel, Word) ca și context în cadrul sistemului de management al documentelor.
7. Sistemul trebuie să ofere capacitatea de a transfera date între sisteme care utilizează formate cunoscute de schimb de date.
8. Soluția trebuie să suporte mai multe metode de integrare (de exemplu: WS SOAP, REST API, MQ, KAFKA, etc.)
9. Soluția trebuie să expună toate informațiile din modelul de date prin API.
10. Toate datele gestionate de sistem trebuie să fie disponibile pentru integrare utilizând acces prin API-uri.
11. Sistemul trebuie să ofere capacitatea de a integra seturi de instrumente care să permită proiectarea, dezvoltarea, generarea și distribuția raportelor.

### Monitorizare (Monitoring)

1. Furnizorul de soluții trebuie să furnizeze un instrument de monitorizare 24/7/365 pentru soluția generală, inclusiv toate nivelurile infrastructurii.
2. Soluția va trebui să monitorizeze aplicatiile web în regim de 24 ore/zi si 7 zile/săptămână și să detecteze eventualele probleme înainte ca acestea să afecteze utilizatorul final.
3. Sistemul va avea capacitatea de a monitoriza proactiv aplicația și de a susține disponibilitatea infrastructurii prin monitorizarea „tablourilor de bord” și va oferi alerte de monitorizare a performanței care pot fi configurabile și care să permită notificarea utilizatorului folosind mai multe metode de comunicare.
4. Sistemul trebuie să ofere capacitatea de a monitoriza / gestiona toate componentele aplicației dintr-o „consolă” principală, bazată pe web.
5. Sistemul va avea capacitatea de a monitoriza, gestiona și urmări toate tranzacțiile pentru aplicații.
6. Soluția trebuie să dispună de o interfață de utilizator Web intuitivă și fiabilă. Accesul se face pe bază de roluri pentru a permite diferite niveluri de acces și de control atât pentru utilizatori, cât și pentru grupuri de utilizatori.
7. Soluția trebuie să ofere tablouri de bord care conțin date care sunt relevante numai pentru o anumită persoană/grup/rol.
8. Soluția trebuie să suporte nativ monitorizarea serviciilor de rețea.
9. Soluția trebuie să furnizeze mecanisme interne pentru disponibilitate înaltă.
10. Soluția trebuie să ofere posibilitatea criptării transmisiei datelor între componente.
11. Sistemul trebuie să furnizeze API-uri deschise care să permită integrarea ușoară cu alte sisteme informatice.
12. Soluția trebuie să fie capabilă să execute diverse scripturi în cazul apariției unei alerte.
13. Soluția trebuie să permită politici de notificare configurabile, prin care să poată fi definiți destinatarii alertelor în funcție de ora din zi, sursa, eveniment, severitate, etc.
14. Soluția trebuie să trimită notificări prin e-mail despre alerte către utilizatori sau grupuri de utilizatori.
15. Soluția trebuie să furnizeze tablouri de bord standard și tablouri de bord personalizate pentru afișarea corelată a datelor care acoperă infrastructura monitorizată.
16. Accesul și autentificarea utilizatorilor trebuie să fie compatibile cu LDAP.

### Performanță (Performance)

1. Sistemul trebuie să ofere în medie un timp de două (2) secunde timp de raspuns pentru ecran sau tranzacției în momentele de vârf
2. Sistemul nu va diminua timpul de răspuns mediu de două (2) secunde în perioadele de utilizare maximă la executarea interogărilor/rapoartelor salvate și/sau adhoc.
3. Sistemul trebuie să ofere posibilitatea de a administra/controla prioritatea proceselor bazate pe criterii configurabile.
4. Sistemul va oferi capacitatea administratorului de sistem de a urmări performanța și utilizarea. Aceasta ar trebui să includă:
   1. Capacitatea de a urmări și de a înregistra ce utilizatori sau grupuri de utilizatori au cea mai mare utilizare și ce accesează;
   2. Capacitatea de a furniza statistici privind performanța sistemului;
   3. Capacitatea de a urmări și de a se înregistra (logging) care sunt rapoartele sau elementele de bază de date, utilizate cel mai mult.

### Platforma (Platform)

1. Furnizorul de soluții va oferi suport pentru toate mediile, fără excepție (producție, dezvoltare, testare și acceptanță).
2. Sistemul trebuie să ofere capacitatea de a accesa și interoga toate datele conținute în sistem.
3. Sistemul va permite ca output-ul (interogări, rapoarte, diagrame, grafice și hărți) să fie produse de către utilizatorul final în oricare dintre următoarele formate: HTML, PDF, Microsoft Excel, CSV, XML, fișiere cu text lățime fixa și fișiere cu text delimitat, și formatul de ieșire nativ al soluției.
4. Sistemul trebuie să furnizeze toate funcționalitățile utilizatorului final printr-o interfață web de amprentă zero. Utilizatorii finali nu ar trebui să aibă nevoie de software dincolo de un browser web. Soluția nu trebuie să necesite utilizarea unor capacități sau software de browser web specific/proprietar. Soluția nu ar trebui să necesite utilizarea controalelor ActiveX.
5. Sistemul trebuie să ofere capacitatea utilizatorilor de a personaliza interfața de utilizator la setările lor individuale pentru nivelul lor de securitate.
6. Soluția trebuie să fie implementată într-un mediu cu înaltă disponibilitate și load-balancing.

### Programare rulare job-uri (Job Scheduling)

1. Sistemul trebuie să ofere capacitatea de a efectua procese batch.
2. Sistemul trebuie să ofere capacitatea de procesare batch și controale la nivel de interfață:
   1. Reconcilarea între sursă și aplicația țintă pentru a se asigura că transferul de date este complet și corect;
   2. Asigurarea că erorile din timpul procesării interfeței sunt identificate prin procese compensatorii și investigate prompt, corectate și retrimise pentru procesare;
   3. stabilirea unei scheme de confirmare pozitivă pentru a se asigura că fișierele trimise dintr-un sistem sursă sunt primite de sistemul țintă (adică „handshake” între sisteme, astfel încât fișierele să nu fie omise sau pierdute);
   4. asigurarea că fișierele generate de o interfață de aplicație (atât sursă, cât și țintă) sunt securizate corespunzător împotriva accesului și/sau a modificărilor neautorizate;
   5. stabilirea și revizuirea periodică a unui jurnal de procesare a interfeței care captează erori și excepții;
   6. Utilizarea facilităților de eroare și corecție pentru a urmări și corecta erorile în datele din interfață;
   7. Stabilirea și utilizarea unui mecanism (de exemplu, mesaj de e-mail) pentru a notifica utilizatorii atunci când datele sunt respinse. Aceste mesaje ar trebui să se repete zilnic până când sunt corectate;
   8. Asigurarea că fișierele utilizate în schimbul de date sunt arhivate sau șterse automat din mediul de producție după procesare pentru a preveni mai multe iterații de procesare ale acelorași date.

### Securitate (Security)

1. Sistemul respectă cerințele de control și autentificare prevăzute în politica de securitate.
2. Sistemul va utiliza tehnologii de criptare aprobate, cum ar fi FIPS 140-3 (Link: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>).
3. Sistemul va oferi capacitatea de a restricționa toate funcțiile de raportare și interogare pentru aceleași profiluri de securitate, precum și limitările de acces la date aferente ale aplicației de bază.
4. Sistemul trebuie să ofere capacitatea de a accesa toate componentele aplicației prin single sign-on sau login unic.
5. Sistemul trebuie să ofere capacitatea de a avea delimitari puternice (pe niveluri) și documentate între extranet, internet și intranet.
6. Sistemul va oferi administratorilor posibilitatea de a restricționa accesul la date în funcție de rol, grup sau utilizator pe baza definiției rolului de securitate.
7. Sistemul va oferi administratorilor posibilitatea de a restricționa accesul la date pe baza de adresa IP și intervale de adrese.
8. Sistemul trebuie să ofere administratorilor posibilitatea de a restricționa accesul la date la nivel de câmp al ecranului/paginii, tipul de meniu și tipul de tranzacție.
9. Sistemul va oferi capacitatea administratorului de a restricționa accesul la date după tipul raportului.
10. Sistemul trebuie să ofere administratorilor posibilitatea de a restricționa accesul la date la nivel de tabelă de bază de date.
11. Sistemul va oferi administratorilor posibilitatea de a defini profilurile de securitate care restricționează capacitatea utilizatorului de a se conecta.
12. Sistemul trebuie să ofere administratorilor posibilitatea de a defini profilurile de securitate care restricționează capacitatea utilizatorului de a adăuga/modifica/șterge/actualiza și vizualiza datele.
13. Sistemul oferă capacitatea de a permite administratorilor să vizualizeze sau să obțină rapoarte de securitate care arată utilizarea sistemului autorizat/neautorizat.
14. Sistemul va oferi capacitatea de a genera un mesaj de avertizare pentru a notifica administratorul dacă mai multe profiluri de securitate aplicate unui singur utilizator sunt în conflict.
15. Sistemul trebuie să ofere capacitatea de a data cu data efectivă toate adăugările, ștergerile, actualizările și modificările la setările și parametrii de securitate.
16. Sistemul trebuie să ofere capacitatea de a asigura transmiterea parolelor folosind protocoale/algoritmi siguri.
17. Sistemul va oferi capacitatea de a defini grupurile de acces ale utilizatorilor pe baza responsabilităților pentru a asigura segregarea atributiilor.
18. Sistemul trebuie să ofere capacitatea de a întreține fișierele de configurare legate de parolă și securitate într-un depozit/container criptat.
19. Sistemul trebuie să ofere capacitatea de a izola sesiunile, astfel încât o eroare într-o singură sesiune să nu afecteze alte sesiuni.
20. Sistemul va oferi capacitatea de a dezactiva automat un ID de conectare a utilizatorului după o perioadă de inactivitate definită de administrator.
21. Sistemul trebuie să ofere administratorilor posibilitatea de a defini caracteristicile necesare parolei.
22. Sistemul trebuie să ofere administratorilor posibilitatea de a restricționa accesul la date pentru fiecare profil de securitate, în funcție de modulul de aplicație.
23. Sistemul trebuie să susțină securitatea ierarhică, bazată pe roluri pentru vizualizarea și editarea accesului pentru toate tranzacțiile, interogările și rapoartele.
24. Sistemul va controla crearea, afișarea și schimbarea accesului la tranzacțiile din sistem și va permite alocarea definită de utilizator a acestor privilegii în mod specific tranzacției.
25. Sistemul trebuie să ofere capacitatea de a securiza tranzacțiile și atașamentele ca „read-only”.
26. Sistemul va oferi capacitatea de creare a regulilor de securitate care să asigure:
    1. Controlul accesului pentru grupuri de utilizatori
    2. Controlul accesului pentru utilizatori individuali
27. Sistemul trebuie să furnizeze un model de securitate comun care să fie utilizat de toate componentele. Soluția trebuie să aplice regulile de securitate ale rolului/funcțiilor, indiferent de interfața utilizată pentru toți utilizatorii. Soluția trebuie să aplice regulile de autentificare și autorizare în orice moment și să împiedice ocolirea securității prin apeluri directe sau acces direct prin link/URL.
28. Sistemul trebuie să ofere capacitatea de a adapta automat conținutul prezentat fiecărui utilizator pe baza profilului de securitate al acestuia.
29. Principiile de dezvoltare a aplicațiilor web respectă ghidurile de dezvoltare de securitate ale OWASP și sunt verificate împotriva OWASP Top 10 API, OWASP ASVS.
30. Soluția trebuie să susțină integrarea cu sistemul existent de SSO al Ministerului Finantelor (prin mijloace standard).
31. Solutia trebuie să permită implementarea unui mecanism de tip SSO (Single Sign On)
32. Furnizorul de soluții va dezvolta firewall sau alte mecanisme de protecție a nivelurilor de securitate cu capacitatea de (1) evaluarea adreselor de rețea sursă și destinație și (2) să compare cererea (inclusiv porturile de destinație) cu listele de control de acces predefinite în scopuri de filtrare.
33. Furnizorul de soluții va stabili proceduri pentru a proteja documentele, media computerizată, informațiile/datele și documentația împotriva dezvăluirii, modificării, eliminării și distrugerii neautorizate.
34. Furnizorul de soluții va implementa monitorizarea nivelului de securitate, inclusiv detectarea intruziunilor, testarea penetrării și analiza încălcării masurilor de securitate.

## Cerințe non-funcționale core banking

### Capacitate (Capacity)

1. Furnizorul de soluții trebuie să dimensioneze arhitectura infrastructurii și să demonstreze prin testarea sarcinii și a stresului că sistemul are un comportament stabil în caz de vârfuri de sarcină.
2. Sistemul trebuie să ofere capacitatea de a se adapta la o creștere / an anticipată de 10% a înrolarii de noi utilizatori fără modificări majore ale sistemului sau degradare a performanței pe un orizont de timp de 5 ani.
3. Sistemul trebuie să ofere capacitatea de a se adapta la o creștere / an anticipată de 20% a volumului de date, fără modificări majore ale sistemului sau degradare a performanței pe un orizont de timp de 5 ani.

### Colectare date (Data Entry)

1. Sistemul trebuie să ofere capacitatea de a permite crearea de formulare (UI) personalizate cu completare automată.
2. Sistemul trebuie să ofere capacitatea de a permite fonturi colorate în formulare (UI) care sa fie afișate ca atare pe ecran.
3. Sistemul trebuie să ofere capacitatea de a crește/ scădea dimensiunea fontului în funcție de preferința utilizatorului.
4. Sistemul trebuie să ofere capacitatea de a colecta și recupera datele aplicației, cu controale pentru verificarea integrității referențiale a datelor.
5. Sistemul trebuie să ofere capacitatea de a limita accesul la date pe bază de profiluri de securitate în conformitate cu cerințele și controalele sistemului, în functie de datele care trebuie introduse de utilizator.

### Dezvoltare (Development)

1. Sistemul trebuie să ofere capacitatea de a permite o duplicare separată și completă a software-ului din sistemul de producție (crearea unei copii complete a software-ului), precum și crearea mai multor medii de dezvoltare și testare.
2. Sistemul trebuie să fie compatibil cu framework-urile uzuale/comune/populare de integrare.
3. Sistemul trebuie să ofere capabilitati de servicii Web, care sa fie compatibile cu standardele W3C, inclusiv, dar fără a se limita la SOAP, UDDI, WSDL, REST.
4. Sistemul trebuie să ofere capacitatea de a crea obiecte personalizate, cum ar fi machete, câmpuri, ecrane.
5. Sistemul trebuie să ofere capacitatea de a modifica/schimba obiecte cum ar fi câmpuri și ecrane.
6. Sistemul trebuie să ofere capacitatea de a permite identificarea/raportarea obiectelor definite de utilizator.
7. Sistemul trebuie să ofere capacitatea de a include obiecte definite de utilizator în procesul de upgrade.

### Metadate (Metadata)

1. Furnizorul de soluții oferă un depozit comun de metadate centralizat. Depozitul de metadate ar trebui să întrețină informații despre obiectele, elementele, formulele și filtrele disponibile pentru atribute, șabloane de raport și calendarele de execuție a job-urilor.
2. Sistemul trebuie să ofere capacitatea de a avea un model comun de metadate care poate fi utilizat și valorificat de toate componentele într-o manieră care să permită dezvoltatorilor și administratorilor să facă schimbări/modificari centralizat, într-o singură locație. Modificările ar trebui să fie propagate automat și să fie disponibile pentru utilizare de către toți utilizatorii.
3. Sistemul furnizează capacități de raportare a metadatelor, de ex. Navigarea metadatelor păstrate, cum ar fi definițiile unor rapoarte, funcțiile, parametrii sau analiza dependențelor.
4. Sistemul furnizează capacități de analiză a impactului metadatelor.

### Raportare (Reporting)

1. Sistemul va oferi capacitatea de a crea și de a genera rapoarte ad-hoc de către utilizatorii finali.
2. Sistemul trebuie să ofere capacitatea de a salva definițiile raportului ad-hoc/interogarii.
3. Sistemul oferă capacitatea de a modifica interogările din rapoarte de către utilizatorii finali, cu nivel de securitate adecvată.
4. Sistemul trebuie să ofere capacitatea de a salva rezultatele raportului ad-hoc de către utilizatorii finali.
5. Sistemul trebuie să ofere capacitatea de a include în rapoarte orice valori sau intervale de parametri definite de utilizator (user-defined).
6. Sistemul trebuie să ofere capacitatea de a crea rapoarte care pot include titluri și chenare definite de utilizatorul final.
7. Sistemul va oferi capacitatea de a filtra rapoartele pe baza criteriilor definite de utilizator.
8. Sistemul trebuie să ofere capacitatea de a crea rapoarte din care pot fi suprimate sau tiparite informații pe baza permisiunilor de acces definite pentru utilizator.
9. Sistemul va oferi utilizatorului final posibilitatea de definire a criteriilor de raportare/interogare, cum ar fi, dar fără a se limita la wildcards, căutări de text.
10. Sistemul trebuie să ofere capacitatea de a defini limite de timp în care un raport operațional sau o interogare pot fi executate, precum și numărul de înregistrări care trebuie preluat.
11. Sistemul trebuie să ofere capacitatea de a defini limitele pentru alte tipuri de funcții de interogare, cum ar fi, dar fără a se limita la numărul de "table joins".
12. Sistemul trebuie să ofere capacitatea de a extinde sau constrânge (drill-up / drill-down) o ierarhie definită de date prin intermediul GUI-ului web.
13. Sistemul oferă capacitatea de a genera, publica, converti și distribui rapoarte operaționale în diferite formate.
14. Sistemul furnizează șabloane standard de raportare operațională ad-hoc și va permite utilizatorilor să creeze noi șabloane de raportare.
15. Sistemul trebuie sa genereze rapoarte operaționale declanșate de servicii API.
16. Sistemul va avea capacitatea de a accesa/extrage date pentru analiză.
17. Sistemul trebuie să furnizeze o interfață grafică de utilizator care permite utilizatorilor finali să creeze interogări noi (și să modifice interogări existente) printr-un proces de drag&drop. Interfața de utilizator trebuie să afișeze o listă de obiecte definite care pot fi incluse în interogare ca elemente rezultate și filtre. Utilizatorii finali nu trebuie să fie obligați să introducă sintaxa SQL pentru a crea interogări.
18. Sistemul trebuie să ofere capacitatea utilizatorilor de a transforma cu ușurință orice interogări ad-hoc au creat în rapoarte.
19. Sistemul trebuie să ofere capacitatea de a organiza rapoarte și interogări cu descriere și tag-uri în directoare personalizate și folder.
20. Rapoartele vor putea fi construite pe diverse surse de date, de pe platforme diferite (Oracle, SQL Server, DB2, SQL Anywhere, etc.), în mod transparent pentru utilizatorul final. Rapoartele vor putea fi construite pe un număr variabil de interogări, fără sa fie limitat numărul de astfel de interogări.
21. Soluția ofertată trebuie să permită accesarea în acelaşi timp a bazelor de date
22. Sistemul va permite interfețe cu instrumentele ETL (sistemul va furniza date care urmează să fie extrase, transformate și încărcate în depozitul de date al sistemului).
23. Sistemul trebuie să conțină mecanisme specifice de interfațare cu depozitul de date al sistemului pentru recuperarea informațiilor despre clienți/tranzacții.
24. Componenta de raportare și analize manageriale nu trebuie să limiteze accesul utilizatorilor la o singură sursă de date, permițând combinarea rezultatelor obținute de pe platforme diferite la momentul interogării, astfel încât setul de date rezultat să fie unitar. Pentru funcționare optimă, componenta de business intelligence trebuie să folosească capabilitățile bazelor de date sursă, fără a necesita replicarea datelor pe un server suplimentar și să implementeze un mecanism de generare a interogărilor care să țină seama de tehnologia de baze de date accesată.
25. Utilizatorii sistemului vor putea fi preluați din sisteme LDAP, însă componenta de raportare va trebuie să ofere capabilități proprii de definire a rolurilor pentru restricționarea în detaliu a accesului la rapoarte.
26. Componenta de raportare va permite implementarea unui mecanism de securitate la nivel de înregistrare, permițând utilizatorilor să acceseze doar informațiile specifice structurii din care fac parte.
27. Componenta de raportare trebuie să ofere un mecanism de programare a execuției rapoartelor sau a preîncărcării în zona de memorie cache, astfel încât să minimizeze timpii de execuție ai interogărilor analitice, în funcție de sursele de date.
28. Componenta de raportare va oferi funcționalități de caching care să permită stocarea rezultatelor interogărilor într-o zona de cache urmând ca interogările ulterioare ale utilizatorilor care referă același set de date sau un subset al acestuia să fie servite din zona de cache, fără a mai accesa baza de date sursă. Pentru gestionarea memoriei cache, sistemul va trebui să ofere posibilitatea de a reactualiza, manual sau automat memoria cache, astfel încât să reflecte modificările survenite în bazele de date accesate.
29. Componenta de raportare va oferi posibilitatea de a defini alerte care vor fi executate automat de către sistem.
30. Informația va putea fi consumată prin implementarea unor mecanisme de tip „push” (sistemul va trimite automat, prin canalele de comunicație stabilite, rapoartele generate) sau „pull” (sistemul va genera rapoartele și le va stoca fizic, utilizatorul putând accesa oricând rapoartele dorite). În ceea ce priveste livrarea rapoartelor, aceasta trebuie să se facă :
    1. sincron – generează pe loc documentul în urma lansării unei cereri;
    2. asincron – primește cererea /setul de cereri și apoi generează documentele asociate și le trimite canalului ce l-a solicitat.
31. Componenta de raportare trebuie să ofere posibilitatea programării generării de documente, stabilindu-se momentul rulării, periodicitatea (zilnic, săptămânal, lunar), canalul de livrare a rezultatului (mail, imprimantă, FTP, etc.).
32. Din punct de vedere al surselor de date, componenta de raportare cu format fix va trebui sa permită accesarea informației din surse de date de tehnologii diferite cum ar fi:
    1. baze de date relaționale: SQL Server, Oracle, DB2, etc.
    2. baze de date multidimensionale: SQL Analysis Services, Oracle OLAP, etc.
    3. Servicii Web.
33. Sistemul are capacitatea de a genera rapoarte în paralel, indiferent dacă este vorba de rapoarte de același fel (de ex.: extrase de cont pentru diferiți clienți ai Trezoreriei) sau de rapoarte diferite
34. Sistemul are capacitatea de a ajusta permanent procesarea în paralel, astfel încât să utilizeze optim resursele hardware (de ex.: să nu existe cozi de așteptare pe unele fire de execuție și lipsă de activitate pe altele)

### Raportare Operațională (Operational Reporting)

1. Sistemul trebuie să furnizeze o interfață grafică pentru utilizatori pentru a specifica aspectul raportului și opțiunile de formatare. Utilizatorii finali trebuie să poată adăuga, muta și șterge coloane, specifica sortări de rânduri, specifica grupări de rânduri și modifica alte opțiuni de aspect printr-un drag-and-drop sau o interfață pick-and-click. În plus, utilizatorii finali trebuie să poată adăuga grafice în rapoarte, precum și să adauge text generic pentru a adnota atât grafice, cât și rapoarte.
2. Sistemul trebuie să ofere capacitatea de a permite unor utilizatori cu rol specific de a utiliza SQL direct în loc să utilizeze SQL generat pe baza metadatelor aplicației. Ar trebui să fie posibilă activarea sau dezactivarea aceastei caracteristici la nivel de profil de utilizator.
3. Sistemul trebuie să ofere capacitatea de a extinde sau constrânge (drill-up / drill-down) o ierarhie definită de date prin intermediul GUI-ului web.
4. Sistemul va oferi capacitatea care permite utilizatorilor să editeze și să modifice interogările sau rapoartele existente și apoi să le salveze ca fiind ale lor.
5. Sistemul trebuie să ofere capacitatea de a afișa date într-un format de raport "cross-tabular". Soluția trebuie să permită utilizatorilor să schimbe câmpurile utilizate pentru a produce coloanele și rândurile raportului tabelar încrucișat prin intermediul funcționalității GUI. Soluția nu trebuie să solicite reexecutarea unei interogări a bazei de date pentru a produce o nouă tabelare încrucișată a datelor preluate anterior pentru un raport.
6. Sistemul trebuie să permită unui utilizator să anuleze modificările în aspectul de tabelare încrucișată.
7. Sistemul va permite utilizatorilor să publice o interogare sau un raport finalizat, astfel încât să fie disponibil pentru alți utilizatori.
8. Sistemul trebuie să permită utilizatorilor să salveze o interogare finalizată sau un raport generat cu date, astfel încât acesta să fie static și să nu fie necesară o nouă rulare.
9. Sistemul va oferi capacitatea utilizatorilor și dezvoltatorilor de a crea, salva și publica cu ușurință un nou format de raport (numit și șablon sau layout).
10. Sistemul trebuie să ofere capacitatea de căutare a conținutului la nivel global și local, cum ar fi, dar fără a se limita la raport, domeniul subiectului, tabel, coloană, cuvânt cheie, câmp.
11. Sistemul trebuie să ofere capacitatea de a colabora cu fluxuri de lucru (workflow-uri).
12. Sistemul trebuie să ofere capacitatea de vizualizare a datelor, cum ar fi, dar fără a se limita la pie-charts, grafice.
13. Sistemul trebuie să ofere capacitatea de a avea analitice de BI încorporate în sistemul OLTP.

### Securitate

1. Sistemul va oferi capacitatea de a avea niveluri de securitate pentru a citi, scrie, vizualiza și accesa date pe baza nivelului de ierarhie a organizației, cum ar fi, dar fără a se limita la MF, UTTS, serviciu, compartiment.
2. Sistemul trebuie să ofere capacitatea de a permite administratorului restricționarea accesului la date pentru fiecare profil de securitate la nivel de ecran de aplicație sau de pagină.
3. Sistemul va oferi capacitatea de a permite administratorilor să vizualizeze sau să obțină rapoarte de securitate pe baza profilurilor de securitate.
4. Sistemul trebuie să ofere securitate pentru actualizarea/vizualizarea câmpurilor de date de către utilizator, departament, raport direct, nivel organizațional, etc.

### Utilizabilitate (Usability)

1. Sistemul trebuie să ofere o experiență consistentă, unificată și intuitivă a utilizatorului pe toate interfețele.
2. Sistemul trebuie să ofere capacitatea de a integra mesajele de eroare cu funcția de help on-line.
3. Sistemul trebuie să ofere capacitatea de a asocia funcțiile de ajutor (help) cu tranzacții funcționale la nivel de meniu, ecran, câmp.
4. Sistemul va permite utilizatorilor să trimită rapoarte de eroare a sistemului (definite automat sau de administrator) către administratorul aplicației.
5. Sistemul va permite utilizatorilor să acceseze toată documentația de utilizator, cum ar fi, dar fără a se limita la manualele de help online și organizate pe:
   1. Zone funcționale
   2. Tranzacții
6. Sistemul trebuie să includă meniuri de ajutor pentru funcționalitatea sistemului pentru fiecare tranzacție/functie și fereastră, cu text de ajutor standard și personalizabil.
7. Sistemul va oferi funcționalități de căutare avansate, cu posibilitatea de a căuta între grupuri predefinite de tranzacții și tipuri de tranzacții.
8. Sistemul trebuie să furnizeze facilitatea de ajutor online cu următoarele capacități:
   1. Ajutor la nivelul ferestrei
   2. Ajutor la nivel de câmp
   3. Mesaj de eroare Ajutor
   4. Ajutor sensibil la context
   5. Ajutor de hipertext Windows
   6. Ajutor indexat
   7. Wizards, tutors și coaches care să poată să fie definiți
9. Sistemul va furniza capacități pentru mesaje de eroare după cum urmează:
   1. Furnizarea textului de eroare extins la cerere
   2. Indică ce câmp este în eroare prin evidențierea câmpului
   3. Furnizarea de informații despre toate erorile aplicabile după efectuarea modificărilor
   4. Furnizarea de mesaje de eroare personalizabile pentru utilizator Text stocat în tabelele de sistem
10. Sistemul va permite tipărirea oricărei interogări efectuate online.
11. Sistemul va permite capacitatea de căutare a documentelor atașate și capacitatea de a asocia cuvinte cheie cu fiecare document.

## Cerințe non-funcționale Internet Banking

1. Solutia va fi licențiată pentru platforma de productie (atât în CPD, cât și în CSD), dezvoltare, testare și acceptanță.
2. Aplicația trebuie să permită autentificarea utilizatorilor pe baza unor criterii de securitate, treptate, în concordanță cu gama de operațiuni accesată de către clienți.
3. Partea reprezentată de securitate la nivel de acces al utilizatorilor trebuie să fie auditată de către o societate specializată.
4. Aplicația trebuie să permită:
   1. înregistrarea unui număr de minim 800.000 utilizatori de internet banking;
   2. conectarea concurentă a minim 50.000 utilizatori;
   3. efectuarea simultană a peste 50.000 operațiunii;
   4. timpi de răspuns la efectuarea unei operațiuni să fie de maxim 2 secunde.
5. Prin intermediul modulului Internet Banking clienții trebuie să aibă acces la conturile pe care le au deschise la UTTS, utilizând un echipament conectat la rețeaua Internet.
6. Criptarea și autentificarea datelor transmise va fi realizată prin protocol securizat.
7. Soluția trebuie să identifice tipul de terminal prin care utilizatorul accesează funcționalitățile soluției, urmând să livreze către acesta informațiile solicitate în modalitatea cea mai bună pentru vizualizare, în concordanță cu echipamentul de pe care este accesată soluția. Spre exemplu, clientul poate realiza conexiunea de pe PC, PDA sau telefon mobil. Informațiile/operațiunile solicitate trebuie să fie distribuite către client, astfel încât să poată fi vizualizate, în condiții optime, de pe display-ul echipamentului de pe care a fost accesată soluția.
8. Soluţia va respecta un set de cerinţe minime de securitate, referitoare la:
   1. confidenţialitatea şi integritatea comunicaţiilor;
   2. confidenţialitatea şi nonrepudierea tranzacţiilor;
   3. confidenţialitatea şi integritatea datelor;
   4. autenticitatea părţilor care participă la tranzacţii;
   5. protecţia datelor cu caracter personal;
   6. trasabilitatea tranzacţiilor;
   7. continuitatea serviciilor oferite clienţilor;
   8. împiedicarea, detectarea şi monitorizarea accesului neautorizat în sistem;
   9. restaurarea informaţiilor gestionate de sistem în cazul unor calamităţi naturale, evenimente imprevizibile;
   10. gestionarea şi administrarea sistemului informatic;
   11. orice alte activităţi sau măsuri tehnice întreprinse pentru exploatarea în siguranţă a sistemului.
9. Informatiile financiare proprii vor fi obtinute din mai multe sisteme informatice, iar indisponibilitatea unuia dintre acestea NU va împiedica afișarea datelor provenind din componentele disponibile la momentul interogării.
10. Închiderea automată a aplicației client dupa un timp de inactivitate parametrizabil;
11. Securizarea integrității tranzacției clientului.
12. Soluția trebuie să includă mecanisme de securitate, criptare, etc. la nivelul componentelor critice (sistem de operare, managementul bazei de date, aplicație client) în scopul protejării utilizatorilor la încercările de atac/ furt de identitate/ autorizări frauduloase, etc..
13. Arhitectura hardware definită în ofertă trebuie să fie dimensionată astfel încât să asigure funcționarea fără nicio schimbare de configurație in condițiile:
    1. Creșterii numărului de clienți cu 10% pe an, pe o perioadă de 5 ani;
    2. Creșterii numărului de tranzacții cu 10% pe zi în perioadele de vârf;

## Cerințe non-funcționale portal

1. Soluția va avea un portal în zona de intranet pentru accesul utilizatorilor interni
2. Soluția va avea un portal în zona de internet pentru accesul utilizatorilor externi
3. să ofere toate instrumentele necesare pentru construirea și administrarea unui portal, fără a necesita software suplimentar.
4. să ofere facilităti de administrare de conținut pe bază de partajare, colaborare și automatizare de procese
5. să asigure autentificarea unică a utilizatorilor prin intermediul rolurilor și privilegiilor ce vor fi definite și acordate fiecărei persoane în parte. Utilizatorii vor avea acces numai la aplicațiile și documentele pentru care au drepturi alocate.
6. să ofere o vedere unică, consistentă asupra unei game variate de surse de informații și în concordantă cu acțiunile pe care utilizatorul le are de realizat.
7. interfața prezentată utilizatorului după autentificare trebuie să conțină modalitățile de acces strict legate de aplicațiile la care utilizatorul are drepturi de acces, în funcție de drepturile acordate.
8. conținutul accesat prin portal trebuie să fie automat ajustat, pe baza rolurilor predefinite ale utilizatorilor, în funcție de drepturile acordate.
9. interfața accesibilă prin portal va fi în limba română, va fi o interfață grafică cu stil de organizare unitar, indiferent de utilizator și de drepturile alocate acestuia.
10. sistemul trebuie să ofere suport pentru crearea de noi pagini în Portal, astfel încât să se acomodeze informația nouă cu infrastructura existentă.
11. vor fi predefinite mai multe stiluri de organizare și prezentare a paginilor de portal. Dintre aceste stiluri predefinite va fi permisă alegerea unui stil personal de prezentare de către utilizator.
12. utilizatorii trebuie să aibă posibilitatea de a particulariza paginile la care au acces la nivel de conținut, poziționare sau stil, în funcție de drepturile de personalizare acordate.
13. administratorii de portal trebuie să poată controla drepturile utilizatorilor de a particulariza propriile pagini, în funcție de rolul acestora, sau în funcție de regulile definite.
14. portalul trebuie să includa și un instrument pentru administrarea utilizatorilor. Acesta trebuie să realizeze definirea de useri și parole, schimbare parole, gestiune a drepturilor de acces bazat pe grupuri de utilizatori/roluri, astfel încât un utilizator să poată face parte din mai multe grupuri generice de drepturi de acces, alte activități de administrare useri.
15. sistemul de portal trebuie să permită utilizarea profilelor de utilizatori, administratorul putând seta astfel preferințele atât la nivel de profil, grup, cât și la nivel de utilizator. Aceste preferințe specifică atât accesul pe care îl vor avea la diverse porțiuni ale portalului, cât și drepturile asupra acestor zone.
16. utilizatorii și drepturile de acces sunt stocate și gestionate în cadrul unui sistem standard de autentificare unică. Accesul la oricare din aplicațiile componente ale soluției se va face utilizând o autentificare unică la începutul sesiunii de lucru.
17. comunicația cu sistemul de portal (pentru utilizare sau administrare) trebuie să poată fi facută în deplină siguranță din punct de vedere al comunicației și al accesului la servicii (SSL).
18. soluția de portal trebuie să permită delogarea automată – să ofere un mecanism prin care un utilizator să fie delogat, în cazul în care nu a mai efectuat nici o tranzacție într-o perioadă de timp (interval ce trebuie să poată fi setat de administrator).
19. să suporte structuri ierarhice de navigare arborescentă pentru documente.
20. să fie flexibil din punct de vedere al clienților de tip browser, al sistemelor de operare și al suportului pentru bazele de date.
21. să asigure administrarea prin intermediul unui browser web și să suporte delegarea administrării pentru controlul accesului.
22. dezvoltarea portalului să se facă usor, respectând standardele în domeniu. Pentru aceasta soluția trebuie să ofere API-uri bine definite pentru integrarea cu aplicațiile existente, să ofere posibilitatea utilizării serviciilor web pentru a expune date și funcționalități.
23. să ofere posibilitatea de a implementa portalul într-un mediu cluster, având posibilitatea de a realiza balansarea încărcării, fără componente software adiționale.
24. să ofere capabilități de preluare a utilizatorilor pe un alt nod, în cazul unei căderi hardware (fail over).
25. să ofere mecanisme de caching pentru paginile mai des utilizate pentru performanțe ridicate.

## Cerințe non-funcționale soluție de înrolare a utilizatorilor

1. Să permită facilități avansate de lucru cu capturi de documente de tipul: OCR, indexare, recunoaștere coduri cu bare 1D și 2D, etc.. Pentru documentele standardizate (de ex.: BI/CI/Pașaport) să permită extragerea automata de informații (de ex.: Nume, Prenume, Data nașterii, CNP, adresa, etc.) și să le completeze în câmpurile dedicate acestora din interfața utilizatorului
2. Să conțină instrumentele necesare pentru ca utilizatorii MF cu abilități tehnice și de business să poată asigura mentenanța modulului, modificarea funcționalităților existente, precum și dezvoltarea de funcționalități noi
3. Oferta va include o descriere detaliată a procedurii de back-up / restore
4. Oferta va include o descriere detaliată a procedurii de arhivare anuală a datelor
5. Oferta va include instrumentele necesare replicării datelor la Centrul Secundar de Date (CSD) de la Brașov. Soluția de replicare a datelor trebuie să fie certificată de producătorul platformelor software ofertate (baze de date, sistem de operare, etc.).
6. Oferta va include o descriere detaliată a procedurilor de comutare la Centrul Secundar de Date (CSD) și revenire la Centrul Primar de date (CPD) din Bucuresti în regimul "switch over" și "fail over"
7. Accesul utilizatorilor interni se va efectua prin zona de intranet
8. Accesul utilizatorilor externi se va efectua prin zona de internet
9. Pentru utilizatorii externi, furnizorul va dezvolta mecanismele prin care:
   1. se validează identitatea persoanei care dorește să se înroleze
   2. accesul utilizatorilor se face cu respectarea cerințelor de asigurare a confidentialității, disponibilității și integrității informațiilor vehiculate, prin intermediul celor mai noi tehnologii de rezervare, acces și algoritmi de criptare a informației
10. Comunicația între utilizatorul final și serverul de prezentare/aplicație se va face criptat, folosindu-se https (se vor utiliza algoritmi și tehnici de criptare conform celor mai bune practici actuale în domeniu)
11. Replicarea între instanțele și modulele aplicației active în CPD și CSD, se va face de o manieră care să asigure transferul în regim de înaltă disponibilitate, integritate și confidențialitate a datelor
12. Ofertantul va descrie arhitectura hardware a platformei, indicând echipamentele necesare și dimensionarea acestora
13. Oferta va include descrierea caracteristicilor tehnice și a configurațiilor pentru fiecare din echipamentele hardware indicate
14. Oferta va conține descrierea arhitecturii software a soluției, incluzând toate componentele software necesar a fi instalate pentru buna funcționare a acesteia. În cadrul descrierii arhitecturii software se vor preciza echipamentele hardware pe care componentele software vor fi instalate și resursele de care are nevoie fiecare componenta pentru o funcționare optimă; Arhitectura software va include numărul de licențe necesare pentru fiecare componentă indicata și metoda de licențiere
15. Configurarea inițială a platformelor, sistemelor de operare, a serverelor de baza de date și aplicație va fi asigurată de Furnizor
16. Arhitectura propusă pentru mediul de producție va include asigurarea caracteristicilor de "High Availability" și facilități de replicare a datelor la CSD. Soluția de replicare a datelor trebuie să fie certificată de producătorul platformelor software ofertate (baze de date, sistem de operare, etc.)
17. Soluția va avea activate și configurate, atât la nivel de server de baza de date, server de aplicație, sisteme de operare, cât și la nivel de aplicație propriu-zisă, mecanisme native de audit disponibile doar utilizatorilor interni cu atribuții în acest domeniu

## Cerințe componenta de integrare fluxuri

Proiectul va implementa un modul integrat de elaborare de fluxuri electronice (eFlows), ce va avea minim următoarele caracteristici:

1. Va permite profilelor de administratori sau utilizatori ai autorităților competente crearea / modificarea / ștergerea de fluxuri electronice inter-instituționale pentru transferul documentelor sau a altor informații
2. Generarea fluxurilor electronice se va face prin intermediul unui wizard, cu acces restricționat, care va permite minim următoarele funcționalități:
   1. Un flux va avea un punct de început şi unul de sfârșit;
   2. Un flux poate avea unul sau mai multe puncte intermediare de prelucrare
   3. Un flux poate avea ramificații, care vor fi tratate ca sub-fluxuri electronice, cu aceleași caracteristici ca şi fluxurile electronice
3. Crearea de noi fluxuri, cu posibilitatea ca, în mod repetat, să se selecteze de către utilizator, din interfața grafică, tipurile de documente ce vor reprezenta intrări în fluxul electronic

Modulul integrat de elaborare de fluxuri electronice furnizează o infrastructura care elimină orice conexiune directa între consumatorii de servicii și provideri. Consumatorii se conecteaza la bus și nu la providerul care implementeaza efectiv serviciul. Acest tip de conectare decupleaza consumatorul de provider. Modulul integrat de elaborare de fluxuri electronice implementează de asemenea și alte capacități de valoare adaugată. De exemplu, asigurarea securității și a livrării poate fi implementată la nivel central în cadrul bus și nu în aplicații.

Folosirea unui bus ca parte a implementării modulului integrat de elaborare de fluxuri electronice trebuie să permită:

1. Serviciile pot fi refolosite de un număr de consumatori diferiți
2. Să suporte volume mari de interacțiuni individuale
3. Să suporte diferite stiluri de integrare, cum ar fi cele orientate de mesaj sau integrarea pe bază de evenimente (event-driven integration), pentru a lărgi aria de acțiune a modulului integrat de elaborare de fluxuri electronice
4. Să suporte centralizarea Calității Serviciilor la nivel de întreprindere și cerințele privind capacitatea de administrare
5. Modulul integrat de elaborare de fluxuri electronice poate implementa urmatoarele funcții:
   1. Comunicare: nivelul de comunicare pentru a sprijini interacțiunile de servicii. ESB trebuie sa suporte cel puțin SOAP peste HTTP, baza serviciilor web; poate suporta și alte stiluri de comunicare. ESB trebuie să fie capabil să facă direcționarea între stilurile de comunicare (tehnologii) print-un model de numire și administrare unitar
   2. Integrare: conexiune suport pentru o varietate de sisteme care nu sprijină direct interacțiunile de tip servicii, o varietate de servicii poate fi oferită într-un mediu eterogen. Aici sunt incluse sistemele mostenite, aplicațiile pachet și alte tehnologii EAI. Tehnologiile de integrare pot fi protocoale (de ex. JDBC, FTP, EDI) sau adaptoare, precum adaptoarele de resurse pentru Arhitectura Conector J2EE. Trebuie să includa de asemenea invocarea clientului de servicii prin API client pentru diferite limbaje (Java, C+, C#, sau echivalent ) și platforme (J2EE, .Net sau echivalent)
   3. Interacțiunea Serviciilor: sprijină conceptele SOA pentru utilizarea interfețelor, operațiunile de servicii declarative și cerințele de calitatea serviciilor. Trebuie să sprijine modelele de mesaje ale serviciilor corespunzătoare acelor interfețe și să aibă capacitatea de a transmite contextul de interacțiune cerut, cum ar fi securitatea, informatiile privind corelarea tranzacțiilor sau a mesajelor
   4. Disponibilitate ridicată și timp de rulare fault-tolerant, detectarea erorilor și recuperarea tranzacțiilor
   5. Administrare: necesită capacități de administrare în așa fel încât să permită administrarea și monitorizarea pentru a furniza un punct de control al numirii și adresării serviciilor

Managementul modulului integrat de elaborare de fluxuri electronice trebuie să aibă capacitatea de integrare într-un software de management al sistemelor.

## Cerințe platforma de document management (DMS)

Platforma de document management trebuie să ofere următoarele funcționalități, respectiv să respecte următoarele cerințe:

1. Să fie o soluție software care să funcționeze în mod integrat cu platforma eTrezor
2. Sa suporte accesul la documente direct din eTrezor, aplicație desktop sau de pe oricare din browserele web : Microsoft Edge, Google Chrome, Firefox, Safari, Opera, etc.
3. Să permită autentificarea mixta pe bază de nume utilizatori și parola, integrare cu sistemul LDAP
4. Clientul web al modulului DMS să permita salvarea și tipărirea documentelor, precum și transmiterea lor pe e-mail
5. Să permită definirea oricâtor tipuri de documente, indexarea și asocierea de metadate în funcție de care documentele să poată fi ulterior organizate în dosare electronice și în funcție de care să se poată efectua ulterior căutări
6. La captura documentelor să ofere suport nativ pentru oricare din metodele de indexare menționate mai jos:
   1. Indexare manuală – utilizatorul va introduce manual valori în fiecare câmp de indexare
   2. Interogari în baza de date – pe baza valorii unice a unui index , sistemul trebuie să poată popula automat alți indecși asociați, prin interogarea în baza de date a DMS, a eTrezor sau orice alta bază de date utilizată de organizație
   3. Indexare automată dupa șablon – în baza unui șablon configurabil, sistemul să poată automat identifica tipul de document, extrage din fișierul scanat valoarea unuia sau mai multor indecși și salva acești indecși și documente în depozitul central. Extragerea automata de valori aferente indecșilor să permită utilizarea unor reguli de validare, iar în cazul în care aceste reguli de validare nu sunt îndeplinite, utilizatorul să poata fi atenționat chiar la momentul scanării și indexării documentului.
   4. În cazul documentelor care nu au un format predefinit să permită indexarea automată dupa tag-uri (cuvinte cheie și sinonimele acestora)
   5. Să permită recunoașterea automată de tip OCR, ICR, OMR, recunoașterea codurilor de bare, a separatorilor de documente, sau a scrisului de mană lizibil
   6. Să permită generarea de coduri de bare care să fie ulterior folosite pentru indexarea documentelor
   7. Să permită o funcționalitate de tip „Print to DMS” care va permite ca orice document transmisibil spre imprimare să fie încărcat, clasificat și indexat în DMS
   8. Să permită importul documentelor în DMS prin acțiuni simple de tip drag & drop și, în cazul în care acestea sunt puse într-un dosar electronic acestea să moștenească automat metadatele dosarului
   9. Indexarea automata a oricarui document/raport generat din eTrezor și salvarea acestuia în DMS
7. Să permită utilizatorului să selecteze o zona a unui document de tip imagine pentru a extrage automat informații ad-hoc din acea zona și a le completa automat în indecși
8. Să permită gestionarea de revizii și versiuni, precum și compararea de versiuni a documentelor în format editabil cu prezentarea diferențelor
9. Să permită căutarea și regăsirea documentelor în mod concomitent atât după cuvinte cheie (metadate), conținut, cât și note și adnotări asociate documentelor
10. Să ofere capabilități de design de procese/fluxuri de lucru, reprezentabile grafic, cu funcționalități incluse:
    1. de manipulare a documentelor, dosarelor de documente, notelor și indecșilor aferenți
    2. de tip reguli și acțiuni predefinite, suficiente ca și număr și diversitate, astfel încât să poată fi configurate și adaptate fluxurilor de lucru
11. Să permită definirea existenței unui document în fluxul de lucru ca fiind obligatoriu pentru trecerea la pasul următor în proces
12. Să permită trimiterea de notificari pe e-mail către utilizatorii implicați în fluxuri la îndeplinirea anumitor evenimente configurabile
13. Să permită importul atașamentelor din căsuța de e-mail, precum și opțiuni de căutare și regăsire documente direct din aplicația de e-mail. Să permită afișarea documentelor sub forma unor dosare electronice de lucru, preconfigurate sau ad-hoc, dosare organizate pe multiple niveluri ierarhice
14. Afișarea într-un singur ecran a cel puțin următoarelor elemente ale unei înregistrări: vizualizarea conținutului său, metadatele, discuțiile colaborative, notele și adnotările, istoricul cu toată trasabilitatea acțiunilor pe acesta, versiunile, documentele relaționate, fluxurile de lucru pe care se află documentul, precum și comenzile de flux de lucru aferente etapei în care se află acesta, cu posibilitatea de a introduce în același ecran filtre ad-hoc care să permită regăsirea rapidă a informațiilor, conținutului dorit
15. Să permită utilizatorilor posibilitatea de a-și crea propriile interogări
16. Să permită aplicarea de politici automatizate de retenție și arhivare asupra documentelor și dosarelor de înregistrări. Un document o dată îndosariat într-un dosar de tip „înregistrare” să nu mai poată fi editat, extras din dosar sau șters
17. Ștergerea documentelor din depozitul central al platformei de document management să fie de tip logică și nu fizică
18. Să ofere un modul integrat de raportare care să permită rularea unor rapoarte de workflow preconfigurate, exportabile în formate tabelare, dar și posibilitatea de a crea rapoarte adhoc
19. Să ofere funcționalități native pentru configurarea de șabloane pentru generarea rapidă și automată de noi documente în formate standardizate, care să respecte politicile organizației; Aceste documente să poată fi automat încărcate și indexate în DMS alături de informații de la utilizatori („user prompt”) și includerea acestora în documentul nou generat
20. Platforma trebuie să pună la dispoziție un designer nativ de formulare electronice care să permită, folosind metode de tip „wizard”, crearea de formulare de colectare/preluare a datelor, folosind indecși definiți la nivel de document de tip formular. Formularele definite prin platformă trebuie să ofere controale avansate de validare, reguli dinamice, acțiuni, capabilități de calcul formule, de afișare sau nu a unor campuri/controale, în funcție de diverse valori ale unor indecși, câmpuri ale formularului, etapa de workflow sau proprietăți ale utilizatorului. Aceste formulare definite prin designer-ul DMS trebuie să poată fi utilizate atât în modulul DMS, cât și în eTrezor
21. Pentru a asigura protecția automată a datelor cu caracter personal, modulul DMS trebuie să permită funcționalități automate și avansate de » automated redaction » , respectiv să permită configurarea de redacții la nivel de tip de document (imagine), pe bază de șiruri de caractere definite sau expresii regulate. Platforma să permită procesarea documentelor atât în vrac (seturi mari de documente), cât și într-un mod ad-hoc. Procesorul de redactări automate să plaseze adnotări în așteptare pentru redactare în document, vizibile pentru verificare. Utilizatorii desemnați să poată verifica și aproba redacțiile de documente, acestea fiind „arse” permanent în imagine, astfel încât textul selectat să nu mai fie vizibil. Procesul de redactare poate fi, de asemenea, automatizat, fără revizuirea de către utilizator. Funcționalitatea de redactare automată trebuie să permită atât redactarea/arderea permanentă a zonei extrase, dar și salvarea (la cerere) a unei copii a documentului original.
22. Platforma trebuie să suporte facilități de criptare, atât la nivel de bază de date (pentru metadatele aferente documentelor), cât și pentru fișierele stocate pe discurile de stocare aferente platformei sau pentru traficul de rețea
23. Modulul DMS trebuie să pună la dispoziție o componentă centrală de integrare care să asigure comunicarea și interconectarea în timp real și bidirecțional de documente, metadate aferente și evenimente aferente proceselor de lucru (workflow) cu diversele sisteme informatice din cadrul organizației într-un mod configurabil, care să nu presupună scriere de cod custom și să garanteze transferul complet și consistent al informațiilor de orice natura dintre platforma de document management și orice alt sistem, componentă care de asemenea trebuie să permită tratarea și alertarea instantă a erorilor de interconectare
24. Să permită integrarea nativă cu sistemul director propriu (LDAP) pentru preluarea grupurilor de utilizatori și să permită jurnalizarea tuturor activităților utilizatorilor în modulul DMS
25. Să permită delogarea automată a unui utilizator după un interval de inactivitate, interval definit la nivelul fiecărui grup de utilizatori
26. Modulul DMS să permită semnarea electronică și gestionarea documentelor semnate electronic

## Cerințe soluție de disaster recovery

Soluția de disaster recovery propusă trebuie să asigure următoarele caracteristici:

1. Să asigure funcționalități de disaster recovery prin automatizarea și orchestrarea restaurării sistemelor în site-ul de rezervă, în termen de 1 oră
2. Să asigure funcționalități de disaster recovery prin închiderea site-ului principal și pornirea serviciilor în site-ul secundar, în cazul unui pericol iminent identificat
3. Să asigure funcționalități de migrare planificată a site-ului pentru a permite derularea diverselor activități în site-ul principal (mentenanță, relocare, etc.)
4. Să permită rularea de scenarii de testare fără a influența funcționalitatea site-ului principal
5. Să permită, în funcție de caracteristicile mediului de comunicație avut la dispoziție, utilizarea mecanismelor de replicare la nivel mașină virtuala și/sau storage
6. Să fie compatibilă cu soluția de virtualizare ofertată și sistemul să includă licențele necesare pentru realizarea replicării la nivel mașină virtuală peste medii WAN
7. Să fie compatibilă cu soluția de stocare ofertată și sistemul să includă licențele necesare pentru realizarea replicării la nivel storage între site-uri
8. Să fie compatibilă cu soluția de bază de date ofertată și sistemul să includă licențele necesare pentru realizarea replicării la nivel de bază de date

## Estimări de capacitate şi planificare

Soluția va fi proiectată şi construită pentru a răspunde unui volum de date şi de interogări corespunzător, pentru întreaga comunitate de utilizatori.

|  |  |  |
| --- | --- | --- |
|  | Descriere | Estimat |
| 1 | Număr utilizatori interni | 5000 |
|  | Utilizatori interni concurenți | 50% |
| 2 | Număr utilizatori externi | 800.000 |
|  | Utilizatori externi concurenți | 10% |
| 3 | Număr înregistrări anuale | 600.000.000 |
| 4 | Număr conturi analitice | 200.000.000 |
| 5 | Număr înregistrări în zilele cu vârf de sarcină, din care: | 6.500.000 |
| 6 | Număr înregistrări SEP / distriburi / compensări în zilele cu vârf de sarcină: | 4.500.000 |
| 7 | Număr înregistrări operațiuni în numerar / cu cardul la ghișeu în zilele cu vârf de sarcină | 2.000.000 |

## Scalabilitate, disponibilitate ridicată, performanţă

În contextul acestui Caiet de Sarcini, prin scalabilitate se înţelege abilitatea sistemului de a păstra parametrii de disponibilitate, fiabilitate (siguranţă) şi performanţă pe măsura creşterii încărcării.

1. Soluţia trebuie să poată deservi un număr de minim 5.000 de utilizatori interni și un număr minim de 800.000 de utilizatori externi.
2. Soluția trebuie să fie disponibilă 24 ore pe zi; 7 zile pe săptămână; 365 zile pe an. Soluția trebuie să aibă 99.5% disponibilitate.
3. Ofertanţii vor descrie modul în care soluţia, serviciile şi echipamentele oferite vor asigura disponibilitatea eTrezor.
4. Soluția eTrezor va fi proiectată şi construită, astfel încât să fie un sistem scalabil, raportat la dimensiunea bazei de date, volumul de interogări, numărul de utilizatori şi numărul surselor de date.
5. Încărcarea eTrezor poate să crească din diferite motive, incluzând:
   1. creşterea dimensiunii bazei de date
   2. cresterea numărului de înregistrări
   3. creşterea numărului de interogări
   4. creşterea complexităţii interogărilor
   5. creşterea numărului de utilizatori
   6. adăugarea unui număr suplimentar de surse de date
6. Soluția eTrezor va fi construită în aşa fel încât capacitatea sa de procesare să poată fi crescută fără modificarea arhitecturii sale.
7. Ofertanţii vor descrie în propunerea lor modul în care soluţia şi componentele propuse vor adresa cerinţele de scalabilitate şi vor evidenţia eventualele constrângeri. Se vor face referiri la:
   1. Scalabilitatea orizontală – permite creşterea încărcării prin mărirea numărului de servere şi distribuţia încărcării peste acestea
   2. Scalabilitatea verticală – obţinută prin instalarea de software suplimentar pe serverele existente.
8. Prin timp de răspuns se înţelege timpul de răspuns pentru utilizatorul final, mai exact timpul scurs din momentul în care acesta transmite o cerere şi momentul în care primeşte răspunsul.

|  |  |  |
| --- | --- | --- |
|  | Descriere | Actual |
| 1 | Timpul de răspuns - interfața cu utilizatorul (core banking).  Timpul de răspuns nu include timpul de rețea. | ≤ 2 secunde |
| 2 | Timpul de răspuns - interfața cu utilizatorul (internet banking).  Timpul de răspuns nu include timpul de rețea. | ≤ 2 secunde |
| 3 | Timpul de răspuns la cerere (de exemplu: rapoarte complexe).  Timpul de răspuns nu include timpul de rețea. | ≤ 1 minut |

1. Ofertanţii vor indica în răspunsul lor modul în care îşi propun să atingă aceste cerinţe de performanţă.
2. Ofertanţii vor efectua teste (performanță, încărcare, etc.) pentru a demonstra îndeplinirea acestor cerinţe de performanţă, inclusiv cu verificarea numarului de utilizatori concurenti, conform estimarilor de la capitolul [10.9 Estimări de capacitate şi planificare](#_Estimări_de_capacitate)
3. Ofertantul va aduce tool-urile necesare (va pune la dispoziție, cu titlu gratuit) pentru a face teste de performanță, penetrare și teste de stres, care să măsoare și să certifice parametrii de performanță impuși

## Cerințe server web

Componenta pentru redirectarea cererilor trebuie să ofere un framework pentru găzduirea de pagini web statice şi dinamice şi pentru acces la aplicaţii web. Soluţia trebuie să răspundă la cerinţele de mai jos:

1. Componenta trebuie să recepționeze cererile utilizatorilor și să le redirecționeze către aplicațiile corespunzătoare
2. Componenta trebuie să ofere suport pentru comunicații securizate folosind protocoalele actuale Secure Sockets Layer (SSL), Transport Layer Security (TLS) versiune minim 1.3 şi pentru autentificare de bază.
3. Componenta trebuie să permită implementarea unui mecanism de tip SSO în conjuncţie cu soluţia de control al accesului
4. Componenta trebuie să permită implementarea unei arhitecturi de tip PKI
5. Comunicaţiile cu exteriorul reţelei trebuie să se realizeze atât în clar, cât şi criptat, în funcţie de tipul informaţiei; în cazul comunicaţiilor criptate, serverul trebuie să ofere suport pentru SSL
6. Componenta trebuie să permită integrarea cu soluţii de accelerare hardware a criptării/decriptării
7. Componenta pentru redirectarea cererilor trebuie să ofere funcționalități de rescriere a URL-urilor (URL Rewriting) și permită operarea în mod reverse-proxy
8. Componenta pentru redirectarea cererilor trebuie să dispună de mecanisme de balansare a încărcării
9. Componenta trebuie să permită configurarea într-un mod de disponibilitate ridicată
10. Componenta pentru redirectarea cererilor trebuie să ofere suport pentru IPv4 şi IPv6
11. Platforma software de server web de date trebuie să fie disponibilă comercial și va oferi posibilitatea de a rula pe diverse platforme hardware, precum și pe sistemele de operare majore existente pe piață (Windows, Linux și Unix). Nu se admit platforme bazate pe licențiere GPL sau produse customizate special pentru acest proiect. Caracteristicile existente ale produsului trebuie să fie regasite în documente publice.

## Cerințe server de aplicații

Într-o arhitectură, serverul de aplicaţii este cel care expune nivelul logic şi procesele de business, pentru a fi accesate şi utilizate de clienţii soluţiei. Deoarece sistemul informatic este construit pe o arhitectură n-tier cu tehnologii web, sistemul trebuie sa includă clustere de servere de aplicaţii.

Serverul de aplicaţii trebuie să respecte minimal următoarele cerinţe:

1. Platformă tehnologică completă pentru instalarea şi execuţia site-urilor web dinamice, serviciilor web şi aplicaţiilor J2EE sau echivalent
2. Suport complet pentru servicii web utilizând specificaţiile SOAP, JAX-WS si JAX-RPC sau echivalent
3. Securizarea serviciilor web utilizând standardele WS-Security şi WS-SecurityPolicy
4. Mecanisme de grupare a serverelor în clustere de servere de aplicaţii atât în topologii de tip activ-activ, cât şi activ-pasiv
5. Să permită migrarea automată a unei instanțe de server de aplicații dintr-un cluster de pe un nod al clusterului pe altul, conform politicilor de administrare definite
6. Să permită stoparea temporară a unui nod din cluster pentru mentenanţă şi suport, sistemul în acest timp fiind disponibil pentru activităţi normale
7. Mecanisme de scalare a sistemului pe orizontală (Scale Out) şi verticală (Scale Up)
8. Să permită rularea serverului de aplicaţii pe toate distribuţiile majore de sisteme de operare prezente pe piaţă: Windows, Linux şi UNIX
9. Să permită instalarea de noi versiuni ale unei aplicaţii fără întreruperea utilizatorilor conectaţi, asigurând continuitate activăţii de business (Zero-Downtime); vechea aplicaţie va fi dezactivată numai după închiderea tuturor conexiunilor active la momentul instalării noi versiuni
10. Consolă de administrare a serverelor de aplicaţii cu capabilităţi de gestiune a schimbărilor de configuraţii:
    1. blocarea unei configuraţii în vederea modificării
    2. salvarea unei configuraţii fără aplicare efectivă
    3. revenirea la o configuraţie anterioară
    4. istoricul modificărilor
11. Să permită înregistrarea, sub forma unui script de comenzi, a operaţiilor de administrare executate asupra unui domeniu de aplicaţii cu posibilitatea de utilizare ulterioară a acestuia pentru activităţi de administrare si mentenanţă a serverului de aplicaţii
12. Suport pentru protecţie împotriva supraîncărcării serverului de aplicaţii, utilizând opţiuni de configurare a resurselor software pentru cazurile în care serverul nu mai poate accepta noi cereri de procesare, capacitatea maximă a sistemului fiind atinsă
13. Serverul de aplicaţii trebuie să includă facilităţi native de modificare dinamică (self-tunning) a numărului de sesiuni concurente acceptate, în funcţie de gradul de încărcare a sistemului
14. Să ofere mecanisme de balansare dinamică a conexiunilor de date către nodurile unui cluster de componente de gestiune a bazelor de date, în funcţie de încărcarea, disponibilitatea şi timpul de răspuns a sistemelor din cluster; mecanismul trebuie să se bazeze pe funcţionalităţile componentei server de aplicaţii de a capta şi interpreta notificările transmise de componenta de gestiune a bazelor de date referitoare la evenimentele apărute şi gradul de încărcare al nodurilor

## Platforma de securizare a accesului la resurse

Dată fiind importanța asigurării unui grad ridicat de securitate a accesului la informațiile vehiculate prin intermediul interfețelor web ale sistemului, este esențială utilizarea unor soluții avansate de control al accesului web, administrare unitară a conturilor de utilizator și stocare sigură a profilelor. Un alt beneficiu urmărit este facilitarea utilizării sistemului de către utilizatorii care nu au cunoștințe avansate de IT, în condiții de maximă siguranță, atât de pe dispozitive de tip stație de lucru, cât și de pe dispozitive mobile (de exemplu tablete).

Consola de administrare a soluției trebuie să fie disponibilă în limba română.

Componentele de securitate ale soluției trebuie sa ia în considerare adresarea următoarelor cerințe:

1. Soluție de control al accesului:
   1. Soluție centralizată pentru controlul accesului la aplicații web, atât de pe stații de lucru, cât și prin intermediul dispozitivelor mobile (de exemplu tablete)
   2. Autentificare unică pentru toate modulele web ale sistemului
   3. Administrare centralizată a politicilor de acces la aplicații web
   4. Securizarea parolelor (politici de parole avansate)
   5. Schimbarea parolelor utilizatorilor în regim "self-service", folosind un mediu web securizat
   6. integrare pe bază de standarde cu alte sisteme externe care dețin propriile lor depozitare de utilizatori, în scopul asigurării autentificării locale
2. Soluție de stocare sigură a profilelor de utilizator:
   1. De tip LDAP v3 sau superior
   2. Stocarea efectiva a informației să se facă într-o structura de tip bază de date
   3. Informațiile stocate să beneficieze de toate avantajele de redundanță, disponibilitate și securitate de la nivelul bazei de date utilizate
   4. sa includă mecanisme de sincronizare a profilelor de utilizatori cu module externe soluției, fără a necesita licențe suplimentare
3. Soluția propusă trebuie să fie bazată pe module disponibile comercial cu suport din partea producătorului. Nu se admit platforme bazate pe licențiere GPL sau produse customizate special pentru acest proiect. Caracteristicile existente ale produsului trebuie sa fie regăsite în documente publice
4. Funcționalitățile cerute sunt minime și obligatorii, ele trebuind incluse în oferta propusă. Implementarea acestor funcționalități nu trebuie să genereze costuri adiționale de licențiere în plus față de cele prezentate în ofertă

### Soluția de control al accesului și administrare a conturilor de utilizator de portal trebuie să îndeplinească următoarele condiții (minime și obligatorii):

#### Autentificare și autorizare

1. Să impună utilizatorilor autentificarea la accesarea sistemului; fără autentificare și autorizare valabile, utilizatorul nu trebuie să acceseze resursele protejate
2. Să ofere integrare nativă, suportată de producătorul aplicațiilor, cu aplicațiile propuse în cadrul proiectului. Nu se admit platforme bazate pe licențiere GPL sau produse customizate special pentru acest proiect. Caracteristicile existente ale produsului trebuie să fie regăsite în documente publice
3. Să ofere control al accesului bazat pe roluri, în combinație cu alți factori, precum momentul de realizare a cererii de conectare, adresa de rețea de unde provine cererea, grupul din care face parte utilizatorul și orice alt atribut din profilul acestuia (inclusiv atribute special definite, nestandard)
4. Să ofere funcționalități de tip single sign-on (autentificare unică) și single sign-off pentru toate resursele protejate; orice utilizator care se autentifică și este autorizat trebuie să aiba acces la informațiile expuse de sistem fără a i se cere reautentificarea pe parcursul sesiunii, atât timp cât nu există politici care să ceară acest fapt
5. Să ofere autentificare multi nivel combinând orice metode de autentificare disponibile (de exemplu: nume utilizator și parolă, certificat digital, etc.)
6. Sa suporte cel puțin următoarele metode de autentificare:
   1. Nume de utilizator și parolă
   2. Certificate digitale calificate
   3. Certificate digitale necalificate
   4. API-uri de autentificare
7. Să permită configurarea comportamentului standard de blocare sau permisie (refuză acces sau permite acces pentru resursele neprotejate)
8. Suport pentru acces federalizat la resursele expuse de parteneri și suport pentru standardele urmatoare:
   1. SAML
   2. Liberty Alliance
   3. WS-Federation
   4. OAUTH 2.0

#### Auditarea accesului la resurse web

1. Nivelul de auditare trebuie să fie configurabil (succes, nereușită, etc.)
2. Să permită auditarea operațiunilor de autentificare și autorizare pentru resursele protejate
3. Auditarea informației de acces SSO să se realizeze centralizat, în baze de date (se dorește compatibilitate cu sistemul de gestiune a bazelor de date al sistemului, astfel încât să nu se foloseasca mai multe locații de stocare a datelor)
4. Să se integreze cu soluții avansate de raportare și să ofere în mod standard rapoarte pentru datele auditate; să permită exportul rapoartelor în diferite formate (ex: PDF, XLS, etc.)

#### Administrare soluție control acces

1. Să ofere o interfață web pentru administrarea componentelor sistemului
2. Toate politicile de control al accesului trebuie să poată fi definite utilizând interfața web a soluției, fără a necesita cunoștințe de programare sau rularea de scripturi pe server
3. Să permită monitorizarea sesiunilor deschise în sistem, prin intermediul consolei de administrare
4. Să permită administratorilor închiderea sesiunilor utilizatorilor
5. Să permită administratorilor sistemului testarea și simularea politicilor de acces aplicate în sistem, astfel încât comportamentul acestora să fie predictibil

#### Modul pentru resetarea parolei SSO

1. Să permită rularea de fluxuri pentru înregistrarea utilizatorilor, recuperarea și resetarea parolei, înregistrarea în grupuri
2. Interfața expusă către utilizatori (self-service) trebuie să permita vizualizarea și modificarea informațiilor din profil
3. Utilizatorii și administratorii trebuie să poată urmării stadiul unei cereri de acces la resurse în timp real, la orice moment
4. Utilizatorii trebuie să iși poată configura întrebări și răspunsuri cheie pentru resetarea parolelor de acces la resurse dintr-un punct unic
5. Soluția trebuie să ofere delegarea administrării utilizatorilor
6. Să suporte politici avansate de parole: lungime parolă, număr și tipuri de caractere necesare, să împiedice reutilizarea aceleiași parole în mod repetat după expirare, dicționar de parole care nu trebuiesc utilizate
7. Să poată genera parole în mod automat la înregistrarea utilizatorilor

#### Arhitectura soluției de control acces

1. Stocarea configurațiilor și a politicilor de acces la resursele web să se realizeze în baza de date a sistemului, fără a exista nevoia unui depozitar proprietar de date
2. Să permită accesarea simultană a mai multor surse de identități pentru realizarea autentificării și autorizării, fără a implica duplicarea informației sau crearea unui metadirector
3. Toate componentele software ale soluției de control acces trebuie să permită rularea în mod disponibilitate ridicată folosind funcționalități native și fără a necesita echipamente suplimentare
4. Să realizeze criptarea informației transferată între componentele sistemului și clienți (HTTPS, LDAPS, etc.)
5. Soluția de control acces să ofere integrare cu soluția de stocare a utilizatorilor și cu cea de administrare unitară
6. Soluția de control acces să poată fi implementată în următorul mod:
   1. Server central de control acces, care prelucreaza cererile de autentificare, autorizare și auditare, inclusiv pentru accesul folosind dispozitive mobile (de exemplu Android, iOS)
   2. Integrare cu serverele web de tip proxy pentru blocarea tentativelor de acces la resursele protejate; nici o resursă web din interiorul sistemului nu trebuie să poată fi accesată direct din exterior, orice acces realizându-se prin intermediul serverelor web proxy
   3. Integrare cu soluția de stocare a profilelor de utilizator (LDAP)
7. Să expună servicii REST pentru accesul la datele utilizatorilor
8. Soluția trebuie să fie ușor de configurat și administrat:
   1. Să nu necesite mai mult de un depozitar pentru stocarea tuturor informațiilor specifice (bază de date), incluzând roluri, politici, fluxuri de lucru sau date de profil ale utilizatorilor
   2. Să permită înaltă disponibilitate
   3. Să suporte personalizare folosind unelte vizuale, fără a fi nevoie ca administratorii să invețe limbaje de programare specifice produsului

### Stocarea profilelor de utilizatori în cadrul soluției trebuie să se realizeze folosind o soluție care respectă următoarele cerințe:

1. Stocarea utilizatorilor să se realizeze într-un director de utilizatori LDAP v3 sau superior
2. Să permită accesarea datelor despre utilizatori atât din baze de date, cât și din directoare LDAP, cu posibilitatea de agregare selectivă a profilelor și expunerea acestor informații în format LDAP către alte sisteme
3. Să ofere o interfață web de administrare și editare a profilelor de utilizatori
4. Profilele utilizatorilor să poată fi extinse prin adaugarea de noi atribute
5. Să ofere mecanisme de securizare a accesului utilizatorilor la atributele din profil (doar citire, citire și scriere, ștergere, adaugare atribute noi, controlarea accesului la atribute, etc.)
6. Să permită integrarea cu celelalte componente ale sistemului general, astfel încât să existe o singură sursă de utilizatori pentru toate nivelurile aplicative
7. Să ofere un modul de virtualizare a surselor de identități (cel puțin LDAP și baza de date). Sursele virtualizate trebuie să se conecteze fără modificarea sistemelor conectate, iar prin modulul de virtualizare să poată fi prezentate către aplicațiile consumatoare sub formă de date agregate

## Platforma de integrare la nivel de date

Componenta de integrare la nivel de date are rolul de extragere, transformare și încărcare (ETL) a datelor și trebuie să îndeplinească minimal următoarele cerințe:

1. Să poată accesa şi integra date din baze de date diferite: Microsoft SQL Server, IBM DB2, Oracle, MySQL, etc., şi să ofere suport pentru accesarea datelor aflate în fişiere (.txt, .csv, .xml, etc.)
2. Să ofere propriul mecanism de detectare a modificării datelor (Changed Data Capture)
3. Să suporte modalităţi diferite de încărcare a datelor:
   1. încărcare masivă de date (Bulk Load)
   2. încărcare incrementală (Incremental Update)
   3. încărcare a datelor captate printr-un mecanism de detectare a modificării datelor (Changed Data Capture)
4. Aplicaţia să permită definirea şi încorporarea de componente reutilizabile suplimentare
5. Aceste componente trebuie să acopere majoritatea tipurilor de transferuri de date: din fişiere în suport relaţional, între tipuri diferite de baze de date relaţionale (de exemplu între SQL Server sau Oracle şi Fox Pro), etc.
6. Procesele de extracţie, transformare şi încărcare să poată fi definite sub formă declarativă, prin selectarea şi maparea vizuală a tabelelor implicate şi menţionarea componentelor de transfer necesare (pentru optimizarea procesului de dezvoltare)
7. Să permită vizualizarea/modificarea procesului sau codului generat şi reluarea anumitor paşi de proces, astfel încât să se detecteze eventualele erori
8. În cadrul mapărilor de date, să se permită definirea de filtre şi de restricţii asupra câmpurilor implicate
9. Să permită consolidarea paşilor de integrare de date sub forma unor fluxuri cu operatori de loop, ramificare pe baza unor condiţii, etc.
10. În cadrul mapărilor de date, să permită definirea de procese multi-sursă, prin care datele să fie citite din mai multe tabele, și multi-target, caz în care în aceeași mapare informațiile vor fi scrise concomitent în mai multe tabele destinație
11. Să permită, în cadrul unei mapari, ramificarea fluxului de date în funcție de un criteriu definit, astfel încât să poată implementa reguli de transformare diferite pentru ramurile desprinse
12. Să permită definirea de mapări reutilizabile, astfel încât regulile de procesare înglobate într-o astfel de mapare să poată fi reutilizate, ori de câte ori este nevoie, în cadrul altor mapări
13. Să ofere posibilitatea de a depana o mapare prin execuția pas cu pas a transformărilor
14. Să permită notificarea prin e-mail a administratorilor în anumite condiţii de lucru şi să poată întrerupe fluxul de execuţie în cazul unor erori considerate grave
15. Fluxurile definite să poată fi rulate în medii diferite (producţie, dezvoltare, etc.) doar prin selectarea contextului de lucru
16. Să ofere suport pentru web-services
17. Mediul de lucru să nu necesite cunoştinţe avansate de programare
18. Să permită păstrarea istoricului diverselor versiuni ale mapărilor de date
19. Pentru optimizarea proceselor şi a accesului la date soluţia trebuie să se bazeze pe componente reutilizabile, gata construite, de tipul celor mai bune practici, care să încorporeze elemente predefinite pentru consolidarea, asigurarea calităţii şi accesul specific pentru fiecare din tipurile de surse accesate
20. Componentele reutilizabile predefinite pentru accesul datelor trebuie să cuprindă logica necesară extracţiei şi integrării de date, cu toţi paşii ce trebuie parcurşi, inclusiv pentru detectarea modificărilor (mecanism de Change Data Capture) la sursă pentru încărcări incrementale
21. Să suporte mecanisme de tip Slowly Changing Dimensions
22. În cadrul mapărilor trebuie să fie permisă utilizarea unor funcţii native ale bazei de date accesate
23. Pentru funcţionare, modulul de integrare al datelor nu trebuie să necesite un server adiţional faţă de serverele sursă de unde se extrag datele sau serverele destinaţie unde vor fi datele încărcate

## Soluție de securizare a comunicațiilor

1. Soluția de securizare a comunicațiilor va cuprinde:
   1. pentru fiecare din sediile UTTS ce funcționează independent (16 locații) se va realiza redundanță fizică la nivel de echipamente router; Ofertantul va furniza 2 echipamente router pentru fiecare locație.
   2. pentru trezoreria Municipiului București Ofertantul va furniza 6 switch-uri și câte 4 switch-uri pentru celelalte unități de trezorerie din București
   3. pentru UTTS la nivel național (195 locații) Ofertantul va furniza câte 2 buc switch-uri pentru fiecare locație
2. Soluția de securizare a comunicațiilor IP trebuie să îndeplineasca următoarele cerinţe tehnice minimale obligatorii:
   1. Infrastructura ofertată trebuie să beneficieze de o soluție de securizare a comunicațiilor IP de ultimă generație prin intermediul căreia să poată fi asigurate următoarele functionaliăți principale:
      1. Securizarea perimetrală prin implementari de tip Firewall, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam
      2. Criptarea comunicațiilor end-to-end prin implementări VPN IPSec/SSL
      3. Nivel cât mai ridicat de disponibilitate prin utilizarea unor mecanisme automate (ce nu necesită intervenția operatorului uman) de fail-over și rerutarea a traficului IP în cazul defectării componentelor active
      4. Utilizarea unor platforme hardware dedicate pentru:
         1. componentele de securizare perimetrală
         2. componenta de logare și raportare a evenimentelor din rețea
   2. Pentru asigurarea unui nivel cât mai ridicat de integrare și usurință în administrare este necesar ca firewall-urile și platforma de logare și raportare a evenimentelor de securitate să aparțină aceluiași producător. De asemenea serviciile de suport și garanție din partea producătorului trebuie să acopere o perioadă de minim 3 ani (inclusiv pentru servicii de update semnături AV/AB/IPS/URL Filtering/Application Control).

### Echipament router

|  |  |
| --- | --- |
| Specificații tehnice și cerințele funcționale minime pentru Router | |
| R.1 | Router rackabil de 19 inch, maxim 1U, modular, cu toate accesoriile necesare montării în rack |
| R.2 | Minim 8 x interfețe 1 GbE SFP:  Minim 4 x interfete 10 GbE SFP+  Minim 16 x interfete 1 GbE RJ45  Minim 1 x interfață management 10/100/1000 BaseT out of band  Minim 1 x interfață consolă serială  Minim 1 x USB consolă  Echipare cu Minim 2 modul 10 GbE SFP+ SR  Echipare cu Minim 2 modul 10 GbE SFP+ LR |
| R.3 | Minim 2 surse de alimentare 230V AC la 50 Hz (vor fi incluse cabluri de alimentare compatibile cu standardele din România) consum maxim 130 W |
| R.4 | Throughput – minim 15Mpps |
| R.5 | Sesiuni tcp simultane – minim 3.000.000 |
| R.6 | Throughput Firewall IPv4 (64 byte, UDP) – 10 Gbps |
| R.7 | Latență firewall maximă (64 byte, UDP) - 5 μs |
| R.8 | IPSec VPN Throughput (512 byte): minimum 10 Gbps |
| R.9 | IPS Throughput: 5 Gbps  NGFW Throughput: 3 Gbps  Threat Protection Throughput: 3 Gbps  SSL Inspection Throughput: 3 Gbps  Sesiuni Concurente (TCP): 3.000.000  Tunele VPN IPSec Gateway-to-Gateway: 2000  Tunele VPN IPsec Client-to-Gateway : 5000  Instanțe virtuale (licențiate): 10 |
| R.10 | Suport pentru automatizare înnoire certificate digitale – ACME |
| R.11 | Suport pentru captare trafic și vizualizare a traficului captat |
| R.12 | Funcții de rutare:  Multiple WAN support  DHCP Client/Server  Policy-based routing  IPv4/IPv6 dynamic routing: OSPF, BGP, Multicast  VLAN Tagging (802.1q)  Routing between VLANs  Multi-link aggregation (802.3ad)  Multi chassis link aggregation ( MCLAG )  IPv6 support (Firewall, DNS, Transparent, SIP)  Content routing – WCCP,ICAP  NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full NAT, STUN  VXLAN  SIP / H.323 / SCCP  VRRP  Trafic Shaping:  DiffServ support  Bandă garantată/maximă  Shaping după IP |
| R.13 | Funcții securitate:  Routed/Transparent  Identificarea aplicațiilor prin inspectarea traficului  Identificare dispozitive, utilizatori care generează trafic  Inspectare trafic SSL  Policy-based NAT  Granular protection profiles per-policy  IPv6 support  DoS protection  DLP cu blocare fișier după tip și dimensiune |
| R.14 | Funcționalități VPN suportate:  IPSEC/SSL VPN  3DES, AES256 encryption support  Autentificare SHA-1, MD5, SHA-512  Diffie-Hellman Group support: 1, 2, 5, 14  Autentificare Certificat sau PSK  IPSec NAT Traversal  Dead peer detection, Replay detection, Autokey keep-alive for Phase 2 SA |
| R.15 | Administrare cu consolă în linie de comandă (CLI) |
| R.16 | Administrare cu interfață grafică web |
| R.17 | Administrare cu interfață HTTP REST API |
| R.18 | Accesul la administrare prin IPv4 si IPv6 |
| R.19 | Trebuie să suporte autentificare cu:  - Baza de date locală  - Integrare server LDAP/Kerberos/Active Directory  - Integrare server Radius/TACACS+ |
| R.20 | Licența perpetuă pentru 10 instanțe virtuale  Licențe perpetuă pentru activarea tuturor porturilor la capacitate și viteză maximă |
| R.21 | Conține toate accesoriile necesare pentru instalarea și punerea în funcțiune |
| R.22 | Garanție și suport de la producătorul echipamentelor pentru minim 36 luni. Update-urile de software/firmware trebuie să fie oferite cu titlu gratuit pe toată perioada garanției tehnice. Suport hardware(24 ore pe zi, 7 zile pe săptămână, timp de remediere cel mai târziu în două zile lucrătoare) onsite, pe o perioadă de 3 ani, care să garanteze diagnosticarea echipament defect și înlocuirea acestuia, fără costuri suplimentare pentru beneficiar;  Suport software (24 ore pe zi, 7 zile pe săptămână) pe o perioadă de minim 36 luni – cu acces direct la website producător, acoperind dreptul de a face update-uri și mentenanță software la sistemul de operare al echipamentului, ori de câte ori este necesar.  Suport tehnic (24 ore pe zi, 7 zile pe săptămână) pe o perioadă de minim 36 luni – cu acces direct la centrul de suport al producătorului, acoperind dreptul de a deshide tickete/cazuri tehnice ori de câte ori este necesar.  Furnizorul va trebui să facă dovada achiziționării acestor servicii de la producătorul echipamentelor cel mai târziu până la semnarea Procesului verbal de recepție finală. |

### Echipament switch

|  |  |
| --- | --- |
| Specificații tehnice și cerințele funcționale minime pentru Switch tip 1 Layer 2 cu management 24 porturi | |
| S.1 | Switch rackabil de 19 inch, maxim 1U |
| S.2 | Minim 24 x 1 GE RJ45  minim 4 x 10 GbE SFP+  minim 1 x RJ-45 Serial Console Port |
| S.3 | Include kit de instalare în rack de 19 inch cu toate accesoriile necesare instalării și punerii în funcțiune |
| S.4 | Sursa de alimentare 230V AC la 50 Hz (cabluri de alimentare compatibile cu standardele din România) consum maxim 30W |
| S.5 | Switch capacity: minim 125 Gbps |
| S.6 | Latență: maxim 1μs |
| S.7 | Performanțe comutare pachete: minim 180 Mpps |
| S.8 | Are minim 64MB memorie tip flash și minim 512MB memorie tip DRAM |
| S.9 | Suportă "Jumbo Frames" minim 9120 bytes |
| S.10 | Suportă minim 27000 Adrese MAC |
| S.11 | Suportă minim 3500 de VLAN-uri |
| S.12 | Dispune de minim 2MB buffer pachete |
| S.13 | Instanțe Spanning Tree – minim 15 |
| S.14 | Număr linkuri agregate per grup – minim 8 |
| S.15 | Număr de grupuri de linkuri agregate suportate – minim 15 |
| S.16 | Suport pentru MCLAG – multi chassis link aggregation |
| S.17 | Suport pentru Stacking |
| S.18 | Jumbo Frames |
| S.19 | Auto-negociere Port Speed și Duplex |
| S.20 | MDI/MDIX Auto-crossover |
| S.21 | Asigură funcționalitatea pentru protocoalele: Rapid Spanning Tree Protocol RSTP (802.1w), Multiple spanning tree protocol MSTP (802.1s), instanțe MSTP suportate: minim 15; IEEE 802.1D MAC Bridging/STP , STP Root Guard, STP BPDU Guard; Loop guard, Edge Port/Port Fast, IEEE 802.1Q VLAN Tagging  Private VLAN, IEEE 802.3ad Link Aggregation with LACP, Unicast/Multicast traffic balance over trunking port , IEEE 802.1AX Link Aggregation  IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications  IEEE 802.3x Flow Control and Back-pressure, IEEE 802.3 10Base-T  IEEE 802.3u 100Base-TX, IEEE 802.3z 1000Base-SX/LX, IEEE 802.3ab 1000Base-T, IEEE 802.3ae 10 Gigabit Ethernet, IEEE 802.3az Energy Efficient Ethernet, IEEE 802.3bz Multi Gigabit Ethernet, IGMP snooping, IGMP proxy  IGMP querier, LLDP transmit, LLDP-MED, LLDP-MED: ELIN |
| S.22 | porturi SPAN pentru multiplicarea traficului către aplicații monitorizare |
| S.23 | posibilitatea de setare limite min/max pentru linkuri agregate 802.3ad |
| S.24 | posibilitatea de limitare explicită MAC pe port ( sticky MAC ) |
| S.25 | posibilitatea de setare număr adrese MAC învățate per-port |
| S.26 | posibilitate de setare a notificărilor de depășire a limitei numărului de adrese MAC per port și căt timp adresele sunt învățate și sunt salvate |
| S.27 | protecții “furtuni” de broadcast: Storm control/Per-port storm control/Global burst-size control |
| S.28 | posibilitate limitare trafic cu Flow control per port |
| S.29 | posibilitatea restricționării per port a frameurilor 802.1q tagged / untagged |
| S.30 | Suport 802.1p cu priority queuing trunk și WRED |
| S.31 | Suport rezumat al configurărilor queue mappings |
| S.32 | Marcare pachete QoS |
| S.33 | ECN (Explicit congestion Notification ) |
| S.34 | Suportă protocoalele: TACACS+, RADIUS, SSH v1/v2, NTP, SNMP v1/v2/v3, SYSLOG TCP,SNTP,Telnet. |
| S.35 | Funcționalități securitate și vizibilitate: IEEE 802.1X Authentication Port-based  IEEE 802.1X Authentication MAC-based, IEEE 802.1X Guest and Fallback VLAN, IEEE 802.1X MAC Access Bypass (MAB), IEEE 802.1X Dynamic VLAN Assignment, IEEE 802.1ab Link Layer Discovery Protocol (LLDP), IEEE 802.1ab LLDP-MED, IEEE 802.1ae MAC Security (MAC Sec), IEEE 802.1X open auth, IEEE 802.1X EAP pass-through, Flow Export (NetFlow and IPFIX)  sFlow, DHCP-Snooping, Dynamic ARP Inspection |
| S.36 | Permite administrarea și configurarea prin: portul de consolă, CLI, interfața HTTP Rest API, interfața grafică web, Administrare prin echipamentul layer3 la care este conectat, Accesul la administrare prin IPv4 si IPv6, Upgrade imagine sistem prin TFTP/FTP/interfața grafică web, Protocoale de management suportate: Telnet/SSH, HTTP/HTTPS, SNMP v1/v2/v3, SNTP, SYSLOG TCP, Detectarea și notificarea conflictelor de adresare IP  Detectarea și notificarea temperaturii în echipament  Diagnosticarea cablurilor de date conectate în echipament cu procedura TDR ( time-domain reflectometer)  Accesul la echipament se face cu autentificarea locală a utilizatorilor sau pe un server LDAP/RADIUS  Nu sunt acceptate echipamente cu management în cloud |
| S.37 | Conține toate accesoriile necesare pentru instalarea și punerea în funcțiune |
| S.38 | Garanție și suport de la producătorul echipamentelor pentru minim 36 luni. Update-urile de software/firmware trebuie să fie oferite cu titlu gratuit pe toată perioada garanției tehnice. Suport hardware(24 ore pe zi, 7 zile pe săptămână, timp de remediere cel mai târziu în două zile lucrătoare) on site, pe o perioadă de 3 ani, care să garanteze diagnosticarea echipamentului defect și înlocuirea acestuia, fără costuri suplimentare pentru beneficiar. Suport software (24 ore pe zi, 7 zile pe săptămână) pe o perioadă de minim 36 luni – cu acces direct la website producător, acoperind dreptul de a face update-uri și mentenanță software la sistemul de operare al echipamentului, ori de câte ori este necesar. Suport tehnic (24 ore pe zi, 7 zile pe săptămână) pe o perioadă de minim 36 luni – cu acces direct la centrul de suport al producătorului, acoperind dreptul de a deschide tickete/cazuri tehnice ori de câte ori este necesar.  Furnizorul va trebui să facă dovada achiziționării acestor servicii de la producătorul echipamentelor cel mai târziu până la semnarea Procesului verbal de recepție finală. |

### Echipamente dedicate pentru securizare perimetrală (2 bucăți, în configurație redundantă)

1. Caracteristici hardware minimale per echipament:
   1. Firewall throughput (1518 byte UDP): cel puțin 15 Gbps
   2. Conexiuni pe secundă: cel puțin 120,000
   3. Conexiuni concurente: cel puțin 3.000.000
   4. VPN throughput (criptare AES-128): cel puțin 1,5 Gbps
   5. Echipamentul livrat trebuie să dispună de cel puțin:
      1. 5 x 10/100/1000 Base-T Ethernet
      2. Slot disponibil pentru module de rețea ce pot asigura interfețe 1000 Base-T RJ45, 1000 Base-SX sau 1000 Base-LX
      3. 2 x port USB
      4. 1 x port consolă
2. Caracteristici software minimale obligatorii:
   1. Funcționalități: Stateful Inspection, VPN, Identity Awareness, Mobile Access, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam
   2. Funcționare redundantă (VRRP si clustering)
   3. Functionalități Layer2/Layer3: VLAN, IEEE 802.3ad, NAT, RIP, OSPF, BGP, PIM-SM, PIM-SSM, PIM-DM, IGMP v2
   4. Proxy HTTP și HTTPS
   5. Functionare în mod transparent (bridge mode)
3. Soluția propusă trebuie să dispună de mecanisme native și integrate de balansare a sesiunilor către serverele de aplicație. Metodele de balansare disponibile pentru distribuția sesiunilor vor putea fi de tipul round robin, aleator, bazat pe încărcarea serverelor disponibile sau bazat pe timpul de răspuns cel mai scurt
4. Pentru asigurarea politicilor de securitate în ceea ce privește traficul de tip HTTPS, soluția propusă trebuie să permită decriptarea conexiunilor de tip SSL și inspectarea pachetelor atât pentru trafic de tip inbound, cât și pentru trafic de tip outbound. Aceasta funcționalitate trebuie să permită funcționarea selectivă a sesiunilor după URL
5. Garanţia hardware va fi de minim 36 de luni. Garanţia hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect şi înlocuirea acestuia în maxim 3 zile lucratoare, fără alte costuri
6. Suportul software va fi de minim 36 de luni. Se va asigura acces 24x7 în centrul de suport al producatorului, cu posibilitatea raportării problemelor apărute în funcţionare şi solicitarea rezolvării acestora în funcţie de severitate. De asemenea se va asigura dreptul de a face update-uri şi upgrade-uri la toate componentele software (sistem de operare, firmware, etc)

### Echipament dedicat pentru management, logare și raportare

1. Caracteristici hardware minimale obligatorii:
   1. Capacitate de stocare: cel puțin 1 TB
   2. RAM: cel puțin 4 GB
   3. 4 porturi 10/100/1000 Mbps GbE
   4. 1 port consolă
   5. 1 port Gigabit Ethernet pentru management de tip Out-of-band
   6. 2 porturi USB
   7. 350.000 evenimente pe zi
   8. Posibilitatea de stocare a 3.5 GB log-uri pe zi
2. Caracteristici software minimale obligatorii:
   1. Să faciliteze administrarea centralizată a echipamentelor de tip firewall prin intermediul unei interfețe de tip GUI
   2. Să ofere posibilitatea de vizualizare a logurilor, trend-urilor, de urmărire a evenimentelor, să genereze rapoarte și să poată distribui update-uri de software și semnături IPS/AV/AB, etc.
   3. Interfața de vizualizare a log-urilor trebuie să poată afișa toate log-urile de securitate (Firewall, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, Sandboxing) într-un un singur panou, pentru a simplifica procesul de depanare a problemelor de conectivitate pentru o adresă IP
   4. Interfața de vizualizare a log-urilor trebuie să poată crea filtre folosind obiectele predefinite: client, rețele, grupuri, utilizatori
   5. Posibilitatea de blocarea a traficului considerat suspect direct din interfața de monitorizare a sesiunilor active (fără a fi necesară căutarea/identificarea regulii/regulilor ce permit accesul respectiv)
   6. Să includă o Autoritate de Certificare internă X.509, care poate genera certificate pentru firewall-uri și utilizatori și care permite autentificarea în cadrul tunelelor VPN
   7. Comunicaţia dintre firewall şi serverul de management va fi criptată şi bazată pe certificate de tip PKI, emise de autoritatea de certificare locală
   8. Să includă posibilitatea de a folosi autorităţi de certificare externe care acceptă PKCS # 12
   9. Vor fi suportate următoarele scheme de autentificare: tokens (exemplu SecureID), TACACS, RADIUS, şi certificate digitate emise local sau de către autorităţi publice
   10. Trebuie să fie în măsură să dobândească identitatea utilizatorului de la Microsoft Active Directory, fără nici un fel de agent instalat pe controlerele de domeniu
   11. Trebuie să suporte autentificare transparentă Kerberos pentru Single Sign On
   12. Trebuie să suporte utilizarea de grupuri LDAP
   13. Trebuie să aibă o metodă de autentificare bazată pe browser WEB pentru obţinerea identităţii unui utilizator sau a obiectelor din afara domeniului AD
   14. Analiza conformității/complianței:
       1. Să evidențieze configurații neadecvate si breșe de securitate ale configurației de politici
       2. Să ofere recomandări aplicabile pentru îmbunătățirea securității
       3. Să ofere profiluri de bună practică bazate pe reglementările din domeniu
       4. Să poată evalua complianța cu reglementările majore din domeniu
   15. Funcționalități de analiză a log-urilor:
       1. Log-area centralizată trebuie să fie parte a sistemului de management
       2. Să poată capta automat pachete pentru evenimente IPS pentru a facilita colectarea de probe ce pot fi folosite în analize de tip forensic
       3. Să permită exportul de log-uri
       4. Să permită comutarea automată a fișierului care acumulează log-uri, bazat pe o oră programată sau dimensiunea fișierului
       5. Să suporte adăugarea de excepții în IPS direct din înregistrări/log-uri
       6. Transferul log-urilor de pe firewall pe server trebuie să se realizeze în mod securizat pentru a preveni interceptarea (soluția trebuie sa conțina autentificare și criptare)
3. Garanţia hardware va fi de minim 36 de luni. Garanţia hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect şi înlocuirea acestuia în maxim 3 zile lucratoare, fără alte costuri
4. Suportul software va fi de minim 36 de luni. Se va asigura acces 24x7 în centrul de suport al producatorului, cu posibilitatea raportării problemelor apărute în funcţionare şi solicitarea rezolvării acestora în funcţie de severitate. De asemenea se va asigura dreptul de a face update-uri şi upgrade-uri la toate componentele software (sistem de operare, firmware, etc.)

## Soluție hardware-software pentru efectuarea și restaurarea salvărilor de siguranță

Cerințele de la acest subcapitol sunt numai pentru cazul în care sistemul eTrezor nu se poate integra cu [Soluția hardware-software pentru efectuarea și restaurarea salvărilor de siguranță](#_Solutia_hardware-software_pentru) existentă și nu se poate extinde aceasta soluție la nivelul necesităților sistemului eTrezor.

1. Soluția pentru efectuarea și restaurarea salvărilor de siguranță trebuie să fie bazată pe module de aplicații și sisteme hardware ce vor asigura rularea unor procese automate de salvare și restaurare a datelor, protecția directă a aplicațiilor, monitorizarea politicilor de protecție, eficientizarea acestora prin politici avansate de deduplicare și compresie, integrarea nativă cu medii de arhivare pentru păstrarea datelor unice deduplicate pe termen lung, cu asigurarea compatibilității.
2. Soluția trebuie sa asigure compatibilitatea cu tehnologiile descrise la capitolul [5.17 Descrierea situației actuale la nivelul Beneficiarului](#_Descrierea_situatiei_actuale).
3. Planul de salvare și restaurare a datelor propus de către Contractant și agreat de către Autoritatea contractantă va fi diferențiat pe categorii de date, fiecare având propria politică de salvare constând în metoda salvării, frecvența efectuării salvării de siguranță și retenția salvării de siguranță.
4. Arhitectura soluției pentru efectuarea și restaurarea salvărilor de siguranță să fie de tip Disaster Recovery (DR), astfel încât salvările de siguranță să se regăsească în ambele Centre de date. Salvările de siguranță trebuie să poată fi restaurate în oricare dintre cele două Centre de date, indiferent de gravitatea incidentului produs în Centrul de date devenit indisponibil.
5. Soluția oferită trebuie să asigure integrarea hardware și software a următoarelor componente atât la nivelul fiecărui Centru de date, cât și la nivelul ambelor Centre de date:
   1. Platformă pentru efectuarea și restaurarea salvărilor de siguranță – 2 seturi.
   2. Echipament pentru efectuarea salvărilor de siguranță pe disc – 2 buc.
   3. Biblioteci de benzi – 2 buc.
   4. Benzi de date LTO 8 RW - 385 buc.
   5. Benzi de date LTO-8 WORM – 25 buc.
   6. Rack-uri pentru instalarea componentelor hardware

### Platformă pentru efectuarea și restaurarea salvărilor de siguranță

Produsul software sau suita de produse software din cadrul platformei, denumit(e) în continuare „Produsul”, trebuie să asigure rularea proceselor automate de salvare a datelor, protecția directă a aplicațiilor, monitorizarea politicilor de protecție, eficientizarea utilizării spațiului de stocare prin politici avansate de deduplicare și compresie, integrarea nativă cu mediile de arhivare ofertate pentru păstrarea datelor unice deduplicate pe termen lung. Produsul software pentru efectuarea și restaurarea salvărilor de siguranță trebuie să raspundă următoarelor cerințe specifice:

1. Licențierea produsului trebuie să acopere integral componentele Sistemului informatic eTrezor.
2. Licențierea produsului trebuie să fie de tip perpetuu.
3. Modul de licențiere trebuie să permită migrarea licențelor, ulterior achiziției, fără costuri suplimentare, între diferite medii precum Unix, Linux și Windows și între diferite echipamente de stocare.
4. Produsul trebuie să asigure protecția sistemelor fizice și virtualizate, inclusiv la nivelul aplicațiilor care rulează pe acestea.
5. Produsul trebuie să permită configurarea, programarea și restaurarea salvărilor de siguranță pentru bazele de date Oracle la nivelul Oracle RMAN (Recovery Manager).
6. Produsul trebuie să permită configurarea politicilor de protecție în mod independent la nivel de fișier, director, sistem de operare, la nivelul imaginii intregului sistem sau doar pentru o aplicație specifică.
7. Produsul trebuie să poată susține și protecția stațiilor de lucru de tip Microsoft Windows, Linux și MacOS.
8. Produsul va susține deduplicarea datelor la sursă și destinație prin segmentare cu ajustare variabilă, indiferent de tipul de rețea sau protocolul de transfer utilizat.
9. Procesul de deduplicare trebuie să se desfășoare continuu, “inline”, fără stocare temporară a datelor și să fie global indiferent de sursa acestor date.
10. Produsul trebuie să permită ca agenții săi să comunice direct cu echipamentul dedicat stocării datelor salvate, indiferent de tipul rețelei, iar fluxul de date să se desfășoare între sursă și destinație.
11. Produsul trebuie să ofere protecție prin consistență la nivel de fișiere de date, cât și la nivel de aplicație.
12. Produsul trebuie să protejeze sisteme de calcul de tipul Microsoft Windows, Linux CentOS, Red Hat, SuSE, Ubuntu, Oracle Linux, UNIX și Solaris.
13. Produsul trebuie să protejeze prin module dedicate aplicații terțe, inclusiv IBM Lotus Domino, Microsoft SQL, Oracle Database, IBM DB2, MySQL și PostgreSQL.
14. Produsul va permite protejarea oricăror baze de date prin mecanisme native de protecție către echipamentul dedicat stocării salvărilor de siguranță, păstrând capabilitățile de deduplicare și de compresie la sursă.
15. Produsul va oferi posibilitatea protejării serverelor de fișiere în mod direct către echipamentul dedicat stocării salvărilor de siguranță utilizând capabilități de deduplicare și compresie la sursă fără a fi necesară definirea unor politici centralizate.
16. Produsul va permite definirea de politicii de clonare a datelor salvate pentru perioade de retenție lungi către medii externe de tip bandă și către medii de tip cloud sau medii de stocare de tip obiect.
17. Integrarea cu mediile de stocare dedicate arhivării se va face direct fără recompunerea datelor, păstrând segementele unice deduplicate atât în mediul operațional, la nivelul echipamentului de protecție, cât și în cel de arhivare.
18. Produsul va permite ca procesele de salvare să transmită doar noile segmente de date sau cele modificate față de procesul de anterior, către echipamentul dedicat stocării salvărilor de siguranță.
19. Produsul va oferi posibilitatea ca cererile de restaurare operațională să se facă dintr-un set de date complete, tip „full backup set”, indiferent de politicile de protecție definite și fără transfer de date adițional între aplicația de protecție a datelor și echipamentul dedicat stocării salvărilor de siguranță.
20. Transferul datelor de la sursă la destinație trebuie să poată fi criptat, la fel și stocarea segmentelor de date unice, deduplicate, indiferent de politicile de retenție.
21. Produsul trebuie să accelereze procesul de salvare a unui client prin multiplexarea traficului în fluxuri paralele de la sursa datelor la destinație.
22. Produsul trebuie să permită monitorizarea componentelor de salvare și restaurare, deduplicare și stocare a datelor, software și hardware, într-o singură interfață grafică oferită de producător.
23. Funcțiile de monitorizare și analiză vor putea fi extinse asupra unor produse similare de protecție a datelor, inclusiv de la alți producători, prin rapoarte și analize complexe.
24. Produsul trebuie să permită utilizatorilor căutarea de informații după cuvinte cheie în datele salvate și indexate prin intermediului unei interfețe de tip web. Utilizatorul va putea căuta și recupera fișierele ce conțin informațiile căutate direct din interfața de tip web.
25. Replicarea mașinilor virtuale din infrastructura de producție către infrastructura de recuperare în caz de dezastru trebuie să includă capabilități de deduplicare și compresie pentru a eficientiza transferul datelor între Centrele de date.
26. Produsul trebuie să monitorizeze continuu serviciul de replicare a mașinilor virtuale prin indicatori ce monitorizează cantitatea de date replicată, calitatea legăturii dintre Centrele de date, mărimea dimensiunii pachetelor de date, etc.
27. Produsul trebuie să ofere posibilitate de criptare a datelor transferate de la sursă către destinație, precum și stocarea segmentelor de date unice, indiferent de politicile de retenție.
28. Produsul trebuie să includă mecanisme automatizate de tip “disaster recovery” astfel încât catalogul centralizat a politicilor de protecție să cunoască și să poată utiliza datele replicate în sediul distant.
29. Produsul trebuie să permită politici de arhivare pe termen lung ale salvarilor de siguranță direct în echipamentul pentru arhivarea datelor păstrând formatul acestora și accesul pentru restaurare în caz de necesitate.
30. Produsul trebuie să poată replica datele salvate la distanță, într-un sistem similar, transmițând doar segmentele unice de date noi, deduplicate, față de ultimul proces de replicare.
31. Replicarea datelor între Centrele de date trebuie să fie un proces programabil peste rețea, cu posibilitatea de criptare a traficului de date.
32. Produsul trebuie să permită integrarea cu aplicații de monitorizare și control de la alți producători prin interfețe standard de tip REST API.
33. Produsul trebuie să includă și un serviciu de administrare, raportare și urmărire a arhivelor sistemului de mesagerie electronică existent, inclusiv a arhivelor locale.
34. Produsul trebuie să permită arhivarea mesajelor electronice din server-ul de mesagerie electronică, a căsuțelor de jurnalizare și a arhivelor locale ale utilizatorilor.
35. Produsul trebuie să asigure suport pentru standardele Unicode, menționat de către producător în documentația tehnică a produsului, astfel încât orice conținut să poată fi arhivat, indexat, căutabil în arhivă și afișat.
36. Produsul trebuie să permită multiple modele de arhivare bazate pe politici, care pot fi configurate de către utilizator.
37. Produsul trebuie să ofere o interfață de administrare în care administratorul să monitorizeze modul de funcționare a sistemului, să colecteze parametrii de performanță, să detecteze erorile și să definească alerte.
38. Produsul trebuie să ofere posibilitatea de a căuta și restaura mesajele electronice și fisierele atașate prin intermediului unei interfețe dedicate, pentru minim 25.000 utilizatori ai mesageriei electronice. Utilizatorul va putea recupera mesajele electronice căutate în căsuța poștală.
39. Produsul trebuie să ofere capabilități de căutare și arhivare a fișierelor de tip nsf existente pe stațiile clienților sau pe serverele de fișiere din rețea.
40. Produsul trebuie să poată gestiona, prin politici de arhivare, o cantitate de date de tip mesaj electronic de minim 16 TB, pentru minim 25.000 utilizatori ai mesageriei electronice.
41. Produsul trebuie să utilizeze echipamentul pentru stocarea pe disc a salvărilor de siguranțădin cadrul proiectului.
42. Produsul va fi licențiat pentru a descoperi și securiza conținutul din mesageria electronică neconform cu politicile de securitate și de confidențialitate ale MF.
43. Produsul trebuie să ofere posibilitatea administratorilor de a căuta, colecta, analiza și de a exporta mesaje electronice în cadrul unei investigatii autorizate privind neconformități față de politicile de securitate sau de confidențialitate ale MF.

Platforma trebuie să includă echipamentele de calcul pe care aceasta va funcționa cu îndeplinirea cerințelor Caietului de sarcini.

Platforma trebuie să acopere necesitățile CPD și CSD.

### Echipament pentru efectuarea salvărilor de siguranță pe disc

1. Echipamentul pentru stocarea salvărilor de siguranță trebuie să fie integrat, de tip “appliance”, fără posibilitatea de a instala alte aplicații sau sisteme de operare față de cele incluse de producător.
2. Integrarea cu echipamentul dedicat arhivării datelor se va face în mod direct, fără recompunerea datelor, transferand doar segementele unice deduplicate către acesta.
3. Echipamentul trebuie să beneficieze de protecție a discurilor SAS prin RAID 6 și hot spare.
4. Echipamentul trebuie să includă o capacitate utilă de minim 913 TB în configurație RAID6.
5. Echipamentul trebuie să includă minim 4 porturi 10 Gbps Ethernet BaseT, 8 porturi 10 Gbps Ethernet cu conector optic SFP+ și 8 porturi 16 Gbps FC.
6. Echipamentul trebuie să benefieze de cel puțin două surse de alimentare.
7. Echipamentul trebuie să permită susținerea unui număr de 650 fluxuri de date în paralel, de la surse multiple de date, sisteme fizice sau virtualizate și aplicații, cu o performanță de minim 50 TB/h.
8. Echipamentul trebuie să utilizeze un factor global de deduplicare pentru toate datele salvate și/sau arhivate, indiferent de sursă, protocol sau interfața de rețea prin care sunt transferate.
9. Echipamentul trebuie să permită integrarea cu cel puțin următoarele protocoale: NFS, CIFS, VTL, NDMP și OST.
10. Segmentele de date unice salvate în echipamentul dedicat trebuie să poată fi sigilate, protejate față de eventuale acțiuni de ștergere prin intervenții neautorizate.
11. Echipamentul trebuie să susțină mecanisme de protecție și corecție a datelor salvate, a sistemului de fisiere, prin care asigură verificarea continuă a segmentelor de date deduplicate și disponibilitatea pentru restaurarea granulară sau completă a fiecărui proces de salvare finalizat cu succes.
12. Procesul de ștergere a segmentelor de date deduplicate trebuie să se facă în mod automat, fără fereastra de mentenanță, permițând proceselor de salvare și restaurare să se desfășoare continuu.
13. Sistemul trebuie să permită integrarea cu aplicații de monitorizare și control de la alți producători prin integrare cu interfețe standard REST API.
14. Cantitate: 2 bucăți care vor fi distribuite în mod egal între CPD și CSD.
15. Contractorul va livra toate elementele necesare cablării complete pentru echipamentele livrate, de la porturile echipamentelor și până la porturile switch-urilor Ethernet și SAN descrise la capitolul [5.17 Descrierea situației actuale la nivelul Beneficiarului](#_Descrierea_situatiei_actuale), conform standardului Tier 3, aceasta incluzând utilizarea canalului de cablu suspendat existent, patch-panel-uri de fibră optică montate în rack, jgheaburi pentru traversarea cablurilor de fibră optică de la canalul de cablu suspendat către rack-uri, trunk-urile de fibră optică dintre patch-panel-uri, patch-cord-uri de fibră optică, etc.. Acolo unde nu este posibil din cauza unor limitări tehnologice, patch-panel-urile de fibră optică vor fi montate pe canalul de cablu suspendat. Lungimea estimată a trunk-urilor de fibră optică este de cel mult 30 m.
16. Contractorul va furniza toate SFP-urile optice Ethernet și FC necesare interconectării tuturor porturilor echipamentelor cu rețeaua Centrelor de date utilizând switch-urile Ethernet descrise la capitolul [5.17 Descrierea situației actuale la nivelul Beneficiarului](#_Descrierea_situatiei_actuale).

### Biblioteci de benzi

1. 6 unități (drivere) de scriere/citire cu următoarele caracteristici:
   1. Controller FC 8Gbps;
   2. compatibilitate citire/scriere pe benzi de date de tip LTO-8;
   3. suport pentru benzi de date de tip WORM (Write Once Read Many).
2. Minim 187 sloturi licențiate pentru benzi de date.
3. Scalabilitate la minim 20 drive-uri LTO-8.
4. Scalabilitate la minim 260 sloturi pentru benzi.
5. Conectare:
   1. Fiber Channel (FC): minim 12 interfețe 8 Gbps;
   2. Ethernet: minim 2 porturi minim 10/100 Mbps BaseT.
6. Display LCD pentru operare și administrare cel puțin pentru: verificarea stării sistemului, diagnoza hardware și software, jurnale de sistem, configurări, inventariere.
7. Aplicație pentru management cu acces de la distanță prin browser web, prin care se pot efectua cel puțin următoarele operațiuni: verificarea stării sistemului, diagnoza hardware și software, jurnale de sistem, configurări, inventariere, actualizările de microcod.
8. Suport pentru criptare administrată din aplicații externe și din controller-ul intern.
9. Suport pentru Linear Tape File System (LTFS).
10. Criptare minim AES 256-bit.
11. Failover automat pentru porturi și pentru unitățile de scriere/citire.
12. Partiționarea resurselor pentru cel puțin 4 soluții diferite de salvare și restaurare a datelor.
13. Cititor de coduri de bare.
14. Surse redundante de alimentare pentru fiecare unitate controller sau unitate de expansiune cu benzi.
15. Oferta trebuie să includă benzi de curățare și de test compatibile pentru asigurarea funcționării optime a unităților de scriere/citire pentru o perioadă de 3 ani.
16. În cazul în care bibliotecile de benzi sunt rack-abile, atunci acestea vor fi livrate rack-uri dedicate care vor respecta caracteristicile rack-urilor descrise la capitolul [5.17 Descrierea situației actuale la nivelul Beneficiarului](#_Descrierea_situatiei_actuale)
17. În funcție de amplasarea agreată cu Autoritatea contractantă, Contractantul va livra componentele necesare conectării echipamentelor la rețeaua de alimentare cu energie electrică: siguranțe automate (care vor fi montate în tabloul electric), cabluri de curent electric, fișe mobile, prize industriale aparente, cleme SIR etc.
18. Contractorul va livra elementele necesare cablării complete pentru echipamentele livrate, de la porturile echipamentelor și până la porturile switch-urilor Ethernet și SAN descrise la capitolul [5.17 Descrierea situatiei actuale la nivelul Beneficiarului](#_Descrierea_situatiei_actuale), conform standardului Tier 3, aceasta incluzând utilizarea canalului de cablu suspendat existent, patch-panel-uri de fibră optică montate în rack, jgheaburi pentru traversarea cablurilor de fibră optică de la canalul de cablu suspendat către rack-uri, trunk-urile de fibră optică dintre patch-panel-uri, patch-cord-uri de fibră optică, etc.. Acolo unde nu este posibil din cauza unor limitări tehnologice, patch-panel-urile de fibră optică vor fi montate pe canalul de cablu suspendat. Lungimea estimată a trunk-urilor de fibră optică este de cel mult 30 m.
19. Contractorul va furniza toate SFP-urile optice Ethernet și FC necesare interconectării tuturor porturilor echipamentelor cu rețeaua Centrelor de date utilizând switch-urile Ethernet descrise la capitolul [5.17 Descrierea situatiei actuale la nivelul Beneficiarului](#_Descrierea_situatiei_actuale).
20. Cantitate: 2 bucăți care vor fi distribuite în mod egal între CPD și CSD.

### Benzi de date LTO 8 RW

1. Vor fi livrate 385 de benzi de date LTO-8 RW etichetate, cu capacitatea nativă de 12 TB și comprimată de 30 TB compatibile cu bibliotecile de benzi ofertate la capitolul [10.16.3 Biblioteci de benzi](#_Biblioteci_de_benzi).
2. Benzile vor fi distribuite în mod egal între CPD și CSD.

### Benzi de date LTO-8 WORM

1. Vor fi livrate 25 de benzi de date LTO-8 WORM etichetate, cu capacitatea nativă de 12 TB și comprimată de 30 TB compatibile cu bibliotecile de benzi ofertate la capitolul [10.16.3 Biblioteci de benzi](#_Biblioteci_de_benzi).
2. Benzile vor fi distribuite în CSD.

### Rack-uri pentru instalarea componentelor hardware

1. Înălțime pentru montarea echipamentelor: 42U.
2. Înălțime maximă 2020 mm.
3. Lățime pentru montarea echipamentelor: 19”.
4. Lățimea externă: 600mm.
5. Adâncime: 1200mm.
6. Adâncime interioară utilizabilă în concordanță cu produsele ofertate.
7. Lățime utilizabilă în concordanță cu produsele ofertate.
8. Capacitate încărcare: minim 1000Kg.
9. Uși față prevăzute cu butuc și cheie.
10. Uși spate cu deschidere pe mijloc (uși duble), prevăzute cu butuc și cheie.
11. Uși față/spate perforate pentru ventilație în mediu climatizat.
12. Conector pentru împământare.
13. Ofertantul trebuie să livreze kituri de dimensiune 1U pentru blocarea circulației aerului cald din spatele către fața rack-ului pentru spațiile rămase neocupate.
14. În funcție de amplasarea agreată cu Autoritatea contractantă, Contractantul va livra componentele necesare conectării unităților PDU la rețeaua de alimentare cu energie electrică: siguranțe automate (care vor fi montate în tabloul electric), cabluri de curent electric, fișe mobile, prize industriale aparente, cleme SIR etc.
15. Furnizorul va monta în rack unitățile PDU APC AP8853 existente, menționate în capitolul [5.17 Descrierea situatiei actuale la nivelul Beneficiarului](#_Descrierea_situatiei_actuale) și le va conecta la rețeaua de alimentare de alimentare cu energie electrică. Cantitate: va fi livrat un număr corespunzător de rack-uri pentru instalarea tuturor componentelor hardware, care vor fi distribuite în cele două locații CPD și CSD. În cazul în care bibliotecile de benzi sunt rack-abile, vor fi livrate suplimentar rack-uri dedicate și pentru acestea.

## Soluție audit, monitorizare și securitate

1. Soluția va permite colectarea înregistrărilor de audit și monitorizarea întregii infrastructuri informatice a trezoreriei statului, respectiv servere fizice și virtuale, echipamente de rețea, baze de date și aplicații, stații de lucru utilizator, precum și înregistrări de securitate din tehnologiile firewall, IPS, IDS existente.
2. De asemenea, vor fi asigurate funcționalitățile necesare pentru integrarea informațiilor de audit și securitate provenite din sisteme de securitate fizică și sisteme de prevenire a pierderilor de date (tehnologii de control al accesului, tehnologii de control al privilegiilor administrative, tehnologii de securitate pentru bazele de date).
3. Auditul de securitate va asigura automatizarea colectării datelor de audit de pe toate tehnologiile enumerate, va include un modul de alertare operațională în timp real și va furniza o platformă de investigații care să asigure un nivel de securitate optim prin evaluarea proactivă a riscurilor, furnizarea de rapoarte istorice pe orice perioadă de timp și mentinerea unui control activ, permanent.
4. Auditul de securitate va adresa în egala masură serverele, stațiile de lucru, imprimantele și orice alte echipamente pe care nu se poate instala agent. În acest sens, soluția va include servicii server de colectare și normalizare a mesajelor syslog și fluxului Netflow de pe entitățile care pot livra această capabilitate. Va fi posibilă preluarea, normalizarea, corelarea tuturor evenimentelor și mesajelor în cadrul auditului general de securitate și se vor putea impune alerte de securitate relative la aceste platforme.
5. Pentru a adresa cerințele de conformitate definite în cadrul organizației, soluția agreată trebuie să poată îndeplini trei sarcini esențiale:
   1. Setarea unui standard de bază al conformității și securității organizaționale
   2. Urmărirea activității utilizator și agregarea acesteia cu informații de securitate native ale infrastructurilor
   3. Alertarea asupra violărilor de securitate potențiale, atât cele rezultate din activitatea zilnică a utilizatorilor și administratorilor, dar și asupra celor rezultate din analiza tiparelor de intruziuni
6. Soluția trebuie să constituie un real suport pentru organizație în vederea auditului sistemului informatic. Pe baza suportului de produs și a informațiilor furnizate de acesta, responsabilii de securitate vor trebui să poată:
   1. Colecta date din mediul auditat și seta un standard de bază al securității organizaționale
   2. Efectua modificările necesare pentru a acoperi minimul de cerințe de securitate, care ar putea include delegare granulară de drepturi și segregare de responsabilități
   3. Urmări activitatea zilnică a utilizatorilor
   4. Asigura stocarea pe termen lung a tuturor datelor colectate, indiferent de volumul acestora
   5. Pregătirea procedurilor de remediere, în caz de alertare asupra unor posibile devieri de la standard
7. Sistemul va îndeplini toate cerințele funcționale care să asigure auditul complet de securitate și conformitate pentru întreaga infrastructură de aplicații, îndeplinind sarcinile operaționale necesare cu un minim de efort din partea personalului dedicat:
   1. Să furnizeze colectare securizată a log-urilor de evenimente. Securitatea trebuie aplicată la sursa, la destinație și la transport.
   2. Să pastreze online cât mai multe date posibil; să asigure stocarea flexibilă a până la 5 ani de date. Datele odată centralizate, vor fi arhivate, comprimate si semnate digital pentru a garanta integritatea acestora pe toată durata de stocare.
   3. Să furnizeze o consola de raportare inteligentă. Să dispună de un set semnificativ de rapoarte preconfigurate, dar să permita totodată crearea facilă de rapoarte noi. Aceste rapoarte să poată fi redistribuite și exportate în formatele standard (PDF, HTML, XLSX, TXT, CSV, XML)
   4. Să furnizeze un modul de alertare configurabil. Alertele vor fi predefinite sau definite în cadrul implementării, și vor trebui să poată fi mapate pe diverse scenarii; de asemenea, să poată fi definite alerte pe evenimente corelate.
   5. Să furnizeze suport pentru conformitate; să dispuna de mecanisme de răspuns la regulamentele interne și externe, prin monitorizarea accesului la sistemele critice și detectarea activității neobișnuite.
   6. Să furnizeze automatizare completă a proceselor de colectare și normalizare de evenimente
   7. Să monitorizeze activitatea utilizatorilor; să colecteze și să coreleze utilizatori și administratori și să alerteze automat atunci intervin activități anormale
   8. Să asigure integritatea log-urilor. Să poată utiliza zone tampon pe sursele monitorizate, unde evenimentele să fie duplicate la generare, astfel încât să se evite posibilitatea de intervenție umană asupra surselor de log-uri.
   9. Să asigure redundanță funcțională.
   10. Să furnizeze un mecanism de criptare și comprimare a datelor stocate, pentru un timp de retenție nedefinit. Să garanteze printr-un mecanism de semnare digitală că odată stocate, log-urile nu mai pot fi alterate în nici un mod.
   11. Să furnizeze capacități de analiză a anomaliilor pe baza unui algoritm de auto-învățare; să simplifice tendințele activității de sistem și să detecteze incidentele de securitate
   12. Să permită customizarea colectarii și raportării, pe bază de wizard-uri de configurare
   13. Să permită managementul centralizat al agenților (instalarea și dezinstalarea automată și manuală a agenților)

# Descrierea activităților proiectului

## Analiza și proiectarea sistemului eTrezor

1. Consultantul va face o analiză preliminară și de detaliu a sistemului actual al trezoreriei statului privind fiecare proces în parte, implementarea sa actuală și va propune schimbările necesare pentru realizarea proceselor într-un mediu centralizat web.
2. Consultantul, prin reprezentanții săi, va participa la toate întâlnirile periodice de proiect care vor avea ca scop urmarirea în mod constant a desfășurării activităților de analiza și proiectare de detaliu pentru sistemul eTrezor, pentru asigurarea respectării cerinţelor de integrare a sistemului proiectat în sistemul integrat al MF, calitatea soluţiei propuse, completitudinea acesteia în raport cu rezultatele aşteptate.
3. Analiza va avea în vedere, dar nu se va limita numai la:
   1. sistemul existent TREZOR
   2. aplicatiile CashBNR, Cont Tranzitoriu, Dcredite, Dcredite\_BTS, Depterm, Emicert, Ibancls10g, Înrolare Forexebug
   3. alte sisteme cu care sistemul TREZOR schimbă date: Forexebug, sistemele informatice ale ANAF pentru administrarea contribuabililor, DEDOC, FTY-Star, QpayIntegrator, E-popriri
   4. sisteme cu care trebuie să se integreze noul sistem eTrezor
   5. sisteme aflate în implementare sau în diferite stadii de dezvoltare care pot impacta sistemul eTrezor
4. Consultantul va proiecta scenariul de migrare a datelor în noul sistem. În acest sens, Consultantul va parcurge cerințele de migrare / încărcare de date inițiale necesare pentru a pune în funcțiune sistemul eTrezor (inclusiv date istorice).
5. Consultantul va analiza și va propune soluția de arhivare a datelor.
6. Consultantul va propune necesarul de formare și transfer de know-how pentru administratorii sistemului / dezvoltatorii Beneficiarului.
7. Consultantul va analiza și va propune soluția de asigurare a continuității operaționale a sistemului eTrezor în Centrul Secundar de Date.
8. Consultantul va proiecta modulele din cadrul soluției care vor fi dezvoltate, pe baza cerințelor functionale și non-funcționale din caietul de sarcini.
9. Consultanul va elabora Strategia de Cut-Over, care va descrie pașii pentru trecerea în producție a noului sistem eTrezor.
10. Consultantul va analiza mecanismele pentru autentificare, autorizare și securitate existente la MF, și va proiecta soluția eTrezor, astfel încât aceasta să utilizeze și să se integreze cu acestea.

### Rezultate

1. Cerințele documentate complet în cadrul Raportului de analiza și proiectare: procese, fluxuri și tipuri de documente, actori de business - grupuri țintă, cerințe de schimb de date cu alte sisteme și instituții, cerințe referitoare la conversia și migrarea de date din alte surse pentru asigurarea bunei funcționări și a continuității în raportare (nomenclatoare, tipuri de situații de ieșire, etc.), etc.
2. Soluția eTrezor definită în detaliu: proiectarea bazei de date, proiectarea integrării între module / componente / sisteme și a interfețelor cu alte sisteme, definirea rolurilor și drepturilor de acces pentru utilizatori, etc.

### Documente generate

Următoarele livrabile vor fi furnizate de către Consultant şi supuse spre aprobare Beneficiarului:

1. raport de analiză şi proiectare, care va cuprinde cel puțin următoarele informații aferente modelului operațional actual complet și modelului operațional țintă:
   1. diagrame de proces, fluxuri de lucru, informații preluate și validările efectuate
   2. prezentarea machetelor de introducere a datelor (ecrane de interacțiune) și informații de detaliu ale acestora (enumerarea câmpurilor de date, validări aferente acestora, etc.)
   3. informații despre meniurile / submeniurile/ opțiunile aferente ecranelor TREZOR (sistem actual), respectiv componentele sistemului eTrezor (sistem țintă)
   4. necesităţile de raportare specifice Trezoreriei Statului impuse de regulamentele comunitare sau de legislaţia în vigoare din România (de ex. raportările specifice BNR)
2. nomenclatorul situaţiilor de ieşire (rapoartelor) ale sistemului eTrezor
3. nomenclatorul utilizatorilor sistemului eTrezor (inclusiv clienți) - definirea detaliată a utilizatorilor sistemului eTrezor și definirea profilelor acestora, pe baza cărora se stabilește modalitatea de interacțiune cu sistemul informatic (drepturile utilizatorilor)
4. nomenclatorul de operațiuni
5. strategia de cut-over (trecere în producție)
6. planul de recuperare în caz de dezastru
7. raportul de migrare a datelor, care va cuprinde:
   1. planul de migrare, constând din activităţile şi procedurile implicate în scenariul final de migrare
   2. manualul de migrare, reprezentând materialul ce va fi folosit la efectuarea migrării
   3. procedurile de migrare, pe care Consultantul le va aplica la migrare
   4. specificaţiile de format al datelor pentru migrare, constând în cerinţele pe care trebuie să le îndeplinească datele din fiecare sursă de date pentru a putea fi migrate şi integrate în eTrezor

## Construirea soluției pentru sistemul eTrezor

1. Consultantul va construi soluția globală (sistemul eTrezor) pe baza cerintelor funcționale și non-funcționale, integrată cu celelalte sisteme, în conformitate cu concluziile activităților de analiză.
2. Consultantul va construi și va implementa soluția de asigurare a continuității operaționale (DR) a sistemului eTrezor în Centrul Secundar de Date.
3. Pentru toate sistemele / componentele / modulele dezvoltate, Consultantul va livra și documentația aferentă. Documentația trebuie să descrie în detaliu:
   1. ghiduri și manuale de utilizare a componentelor și modulelor dezvoltate, detaliate pe fiecare ecran de interacțiune cu utilizatorul
   2. schimbul de informaţii dintre eTrezor si celelalte sisteme ale MF cu care se integrează
4. Consultantul trebuie să se asigure că:
   1. soluţia dezvoltată îndeplineşte cerinţele care stau la baza construirii sistemului
   2. minimizează impactul trecerii la modul de lucru cu eTrezor, prin informare completă şi continuă asupra stadiilor proiectului şi a eventualelor riscuri sau constrângeri care pot apărea în decursul procesului de implementare
5. Consultantul va asigura serviciile de instalare și configurare pentru mediul de dezvoltare.

### Rezultate

1. cod sursă
2. mediul de dezvoltare este instalat și configurat
3. toate funcționalitățile solicitate prin prezentul Caiet de Sarcini sunt realizate

### Documente generate

1. ghiduri și manuale destinate utilizatorilor sistemului eTrezor (inclusiv clienți), pentru toate componentele acestuia

*Important! Ghidurile de utilizare eTrezor destinate utilizatorilor componentelor sistemului (inclusiv clienți) trebuie să specifice, într-un format uşor de înţeles, toţi paşii care trebuie urmaţi pentru execuţia fluxurilor funcţionale ale sistemului. Acestea nu conţin detalii tehnice. Detaliile funcţionale sunt grupate pe module şi pe procese de business.*

1. ghiduri și manuale destinate admistratorilor de aplicație eTrezor, pentru toate componentele acestuia (întreținerea nomenclatoarelor, generarea și publicarea de rapoarte noi, administrarea rolurilor și utilizatorilor, etc.)
2. Manualul de management al sistemului (instalare, configurare, administrare, salvare-restaurare, securitate, monitorizare, etc.) - manual destinat personalului de specialitate TIC. Acesta trebuie să acopere arhitectura tehnică şi funcţională a tuturor modulelor sistemului eTrezor şi defineşte atât cerinţele fundamentale de funcţionare a eTrezor, cât şi metode de întreţinere zilnică. Acest document trebuie să fie actualizat pentru fiecare nouă versiune a sistemului şi să conţină cel puţin:
   1. versiunea pentru care a fost creat ghidul
   2. instalare
   3. configurarea eTrezor pentru fiecare componentă internă
   4. configurarea eTrezor pentru colaborarea cu sistemele externe
   5. managementul erorilor
   6. documentaţie de administrare a fiecărui modul în parte
   7. salvarea şi restaurarea sistemului
   8. proceduri de comutare între CPD și CSD
   9. proceduri de arhivare
   10. proceduri pentru managementul identității și securitate
3. planul de instalare pentru mediul de producție
4. documentaţie a software-ului comercial / Open source : descrierea completă, atât funcţională, cât şi tehnică a software-ului folosit.
5. documentaţie a software-ului dezvoltat: descrierea completă, atât funcţională, cât şi tehnică, a software-ului dezvoltat pentru sistemul eTrezor. Toate fişierele sursă dezvoltate vor fi distribuite către MF împreună cu documentaţia aferentă, care trebuie să conţină cel puţin:
   1. Descrierea conţinutului şi a funcţiei fiecărui fişier
   2. Descrierea claselor şi obiectelor folosite
   3. Comentarii în cadrul codului; toate comentariile trebuie scrise în limba română şi în acord cu standardele/convenţiile de dezvoltare a codului. Aceste convenţii vor fi folosite pe parcursul întregului proiect, indiferent de stadiul în care se află. Convenţiile de programare trebuie dezvoltate de către ofertant şi agreate împreună cu MF la începutul proiectului.
   4. Descrierea configurării mediului de dezvoltare pentru stațiile de lucru ale personalului de specialitate TIC
6. Structura bazei de date: În acest document trebuie descrisă întreaga structură a bazelor de date eTrezor (ex: tabele, legături între tabele, elemente specifice, semnificaţia tabelelor şi rolul funcţional al fiecăreia, descrierile câmpurilor din fiecare tabelă, etc.)
7. Interfețe cu sistemele externe
8. Descrierea completă a specificaţiilor hardware şi a instrucţiunilor de instalare, configurare, operare şi depanare
9. Notele de versiune: sunt livrate împreună cu fiecare versiune nouă a eTrezor. Acestea sunt adresate de obicei administratorilor de sistem şi trebuie să conţină: lista funcţionalităţilor nou implementate (sau a celor modificate în noua versiune), precondiţii de instalare a versiunii, modificări asupra bazei de date (daca e necesar), modificări de configurare, instrucţiuni de instalare a noii versiuni (instalare manuală şi automată), alte informaţii
10. Întrebări frecvente: reprezintă de obicei o listă de întrebări şi răspunsuri relative la cele mai importante şi mai cerute informaţii despre sistemul eTrezor. Acestea trebuie să fie sub forma unui document separat, livrat împreună cu documentaţia de versiune sau generală de sistem
11. Alte documente tehnice, evaluări, justificări etc.

## Pregătirea mediului de testare

1. Consultantul va pregăti mediul de testare, scenariile de testare și va efectua testele până la parcurgerea cu succes a acestora.
2. Consultantul va parcurge teste individuale, teste pe module, teste de integritate, teste de performanță, teste de stres. Testele de performanţă vor fi parcurse după definitivarea testelor de integritate. Consultantul va redacta scenariile de testare (pe diverse paliere: funcţional, integrare, performanţă) care vor fi validate de către Beneficiar.

### Planificarea testelor

1. La fiecare nivel de testare, se vor derula anumite teste de tip funcţional şi non-funcţional, pe baza unei planificări, care să acopere fazele de pregătire, execuţie şi analiză a rezultatelor testelor. Dacă planificarea se bazează pe supoziţii care se vor schimba pe parcurs, se va ajusta în mod corespunzător şi planificarea.
2. În faza de pregătire a testării, Consultantul va dezvolta planurile detaliate de testare, specificaţiile de testare, va instala/actualiza mediul de testare şi obiectele supuse testării, va stabili criteriile de intrare şi de ieşire, livrabilele şi criteriile de acceptanţă.

### Dezvoltarea şi execuţia testelor

1. Toate testele, cu exceptia celor de acceptanță, vor fi dezvoltate şi executate de Consultant împreuna cu Beneficiarul.

### Coordonarea testelor

1. Testele vor fi coordonate de MF, care va revizui şi aproba planul şi specificaţiile de testare înainte de execuţia efectivă a testelor, va monitoriza efectuarea testelor şi se va asigura de aplicarea procedurilor de management ale testării.

### Managementul testării şi raportării

1. Consultantul şi echipa MF vor defini şi pune în aplicare pe toata durată testării eTrezor, următoarele proceduri de management ale testării:
   1. managementul problemelor
   2. managementul defectelor, folosind un sistem de clasificare a priorităţii şi severităţii defectelor
   3. managementul schimbării
   4. managementul configuraţiei de testare
   5. managementul configuraţiei mediilor de test
   6. urmărirea progresului testării
2. Urmărirea progresului testării va fi raportată folosind următoarele tipuri de rapoarte:
   1. raportul de stare a testelor
   2. raportul de stare a defectelor
   3. raportul de stare a acoperirii testelor planificate
   4. raportul de stare a disponibilităţii mediului de test
   5. raportul cu sumarul executiv al testelor.

### Livrabile din testare

1. Planul master de test - va documenta modul cum Consultantul abordează testarea sistemului eTrezor, activităţile necesare pregătirii şi efectuării testelor, mediile de testare, livrabilele, rolurile şi responsabilităţile pentru testare, procedurile de testare şi metoda de raportare.
2. Planurile de testare - trebuie să descrie în detaliu activităţile de testare planificate, conţinând:
   1. obiectele supuse testării
   2. obiectivele şi perimetrul testelor
   3. cerinţele mediului de testare
   4. funcţiile de testat şi rezultatele aşteptate
   5. abordarea de testare şi tipurile de teste prevăzute
   6. abordarea folosită în crearea/gestionarea datelor de test
   7. succesiunea testelor din matricea testelor, cu dependenţele corespunzătoare
   8. instrumentele de testare
   9. responsabilităţile în procesul de testare
   10. criterii de intrare/ieşire, care să asigure că sunt pregătite condiţiile de începere a testelor planificate, respectiv finalizarea testelor planificate şi eliminarea defectelor
   11. livrabilele implicate
   12. criterii de acceptanţă
3. MF poate solicita modificarea planurilor de testare.
4. Specificaţiile de testare - trebuie să conţină cel puţin:
   1. cazurile de test
   2. descrierea datelor de test, cu referire la datele de intrare şi la baza de date peste care se execută testele
   3. scenariile de test (lanţuri de execuţie a cazurilor de test pentru a simula procese end-to-end)
   4. matricea cerinţelor funcţionale/non-funcţionale, matricea testelor de acoperire a cerinţelor (mapează cazurile de test cu cerinţele)
   5. matricea condiţiilor de test, matricea testelor de acoperire a condiţiilor de test (mapează cazurile de test cu condiţiile de test)
5. MF poate solicita modificarea specificaţiilor de testare.
6. Consultantul va asigura serviciile de instalare și configurare pentru mediul de testare.

### Rezultate

1. Mediul de test este instalat și configurat
2. Testele sunt finalizate

### Documente generate

1. Planul Master de test
2. Planurile de testare
3. Specificatiile de testare
4. Rapoarte de testare

## Instalarea și configurarea infrastructurii hardware și software (licențe software de bază) a sistemului

1. Consultantul va propune și apoi va executa instalările și configurările hardware și software necesare pentru buna implementare și funcționare la parametrii agreați ai soluției eTrezor, precum și alte activități în legătură cu sistemul ce se implementează.

### Rezultate

1. Infrastructura hardware și software este instalată și configurată

### Documente generate

1. Proceduri de instalare și configurare

## Instalarea și configurarea sistemului eTrezor, pe mediul de producție, migrarea datelor și punerea sistemului în funcțiune.

1. Consultantul va pregăti implementarea soluției (conform scenariilor și planului de implementare) și va executa implementarea, inclusiv migrarea datelor, precum și alte activități în legătură cu aceste operațiuni.
2. Consultantul se va asigura că platformele hardware, software şi de comunicaţii alocate sistemului sunt configurate optim, pentru punerea în funcţiune a sistemului.
3. Consultantul va realiza instalarea și configurarea sistemului eTrezor pe mediul de producție.
4. Consultantul va realiza migrarea datelor istorice conform planului de migrare.
5. Consultantul va pune în funcțiune sistemul conform strategiei cut-over.
6. Consultantul împreuna cu Beneficiarul vor organiza serviciile de suport pentru a oferi asistență utilizatorilor finali cu privire la utilizarea sistemului, dupa punerea în funcțiune a acestuia.

### Rezultate

1. Mediul de producție este instalat și configurat
2. Sistemul este funcțional pentru utilizatorii finali
3. Sistemul funcționează la parametrii stabiliţi
4. Datele istorice sunt migrate

### Documente generate

1. Raport de migrare privind serviciile de migrare efectuate
2. Raport de punere în funcțiune a sistemul eTrezor

## Asistarea Beneficiarului în realizarea testelor de acceptanță.

1. Consultantul va instala și configura mediul de acceptanță, care să aibă resurse și parametrii de funcționare asemănători cu mediul de producție.
2. Consultantul va redacta scenariile de testare de acceptanță (UAT – User Acceptance Test) care vor fi validate de Beneficiar. Consultantul împreună cu Beneficiarul vor executa testele în vederea acceptării sistemului pe baza criteriilor de acceptanță stabilite. Testele se vor realiza conform planului de testare agreat.
3. Testele de acceptanță (UAT) vor fi dezvoltate de Consultant și executate împreuna cu Beneficiarul.
4. Testele de performanță, încărcare, acceptanță (UAT) se vor executa pe mediul de acceptanță și/sau producție, în conformitate cu concluziile activităților de analiză.

### Criterii de acceptanţă

1. Criteriile de acceptanţă de la fiecare nivel de testare vor fi stabilite în acord cu MF (vor fi propuse de Consultant şi aprobate de MF), astfel încât să asigure conformitatea execuţiei testelor cu specificaţiile de testare.

### Procedura de acceptanţă

1. Procedura de aprobare a testelor de acceptanţă trebuie să sumarizeze, în cadrul unui raport final de testare, toate activităţile de testare efectuate, rezultatele şi problemele identificate.
2. Acceptanţa testarii sistemului se va realiza prin semnarea raportului final de acceptanţă de către o comisie numita in acest scop.

### Rezultate

1. Mediul de acceptanță este instalat și configurat
2. Testele de performanță, încărcare, acceptanță sunt efectuate

### Documente generate

1. Plan de testare
2. Specificații de testare
3. Rapoarte de testare de acceptanță

## Mentenanță corectivă și adaptivă a sistemului după acceptarea acestuia.

1. Consultantul va asigura, pe o perioadă de 6 luni de la punerea în producție a sistemului eTrezor, servicii de mentenanță, atât pentru corectarea erorilor nedepistate în timpul testărilor, cât și pentru adaptarea sistemului la noi reglementări
2. Consultantul va actualiza documentația aferenta componentelor pe care s-au efectuat modificări
3. Ofertantul va furniza un sistem de helpdesk care să poată implementa SLA-ul agreat și să aibă minim următoarele funcționalități:
   1. Soluția va include o componentă de tip analiza SLA (Service Level Agreement). Componenta trebuie să fie parametrizabilă pe următoarele componente:
      1. Tipuri de entități
      2. Tipuri de aplicații
      3. Tipuri de servicii aflate în suport sau mentenață
   2. Componenta SLA va emite alerte prin e-mail sau push-notification către userii asociați la respectivul incident în contextul în care timpul de răspuns se apropie de final și nu a fost întreprinsă nicio acțiune
   3. Soluția va include o componentă de tip Listener. Componenta trebuie să fie sub formă de serviciu și trebuie să poata accepta cereri de înregistrare automată în serviciul de tiketing pentru mesajele provenite de la aplicațiile core sau de la serverele de aplicație pe care aplicațiile core sunt instalate. Aceasta componentă trebuie sa fie parametrizabilă pe următoarele componente:
      1. Nivelul mesajului de eroare. Acest nivel va fi conținut în mesaj. În cazul în care mesajul are un nivel scazut de eroare acesta va fi doar afișat pentru dispecerii de suport care pot lua decizia de a constitui incident sau nu. În cazul în care tipul mesajului de eroare este ridicat acesta se va înscrie automat în sistemul de incidente
      2. Proveniența mesajului. În cazul În care un sistem nu se mai află sub asistență atunci acest mesaj va fi afișat doar către dispecerul central, iar acesta va lua sau nu decizia de a înscrie incidentul. În cazul îin care sistemul respectiv se află sub asistență incidentul se va înscrie automat
   4. Soluția trebuie să fie portabilă pe orice dispozitiv(Telefon mobil, Tableta, Calculator)
   5. Soluția va conține o componentă de tip “Knowledge Base”, în care operatorii sistemului vor putea salva articole și modalități în care au fost rezolvate incidentele pentru o refolosire ulterioară

### Rezultate

1. Erorile nedepistate în timpul testărilor au fost corectate.
2. Sistemul a fost adaptat conform noilor reglementări.

### Documente generate

1. Documentație actualizată

## Instruire

1. Consultantul va pregati și va derula sesiuni de instruire în raport de grupurile țintă și de submulțimi ale acestora pentru: formatori, utilizatori speciali, administratori de aplicație și de sistem.
2. Consultantul va răspunde de întreaga logistică pentru sesiunile de pregătire în sală: sălile de curs au dotarea necesară, software-ul necesar este instalat şi funcţionează. Răspunde în egală măsură de contractarea de pachete de servicii pentru asigurarea cazării pentru participanţi, asigurarea decontărilor transportului şi diurnei pentru participanţi şi pentru lectori, în conformitate cu reglementările în vigoare, în cazul în care pregătirea are loc în săli de curs.
3. Consultantul poate efectua sesiuni de pregătire la distanță.
4. Pentru a evalua calitatea sesiunilor de instruire, Consultantul va crea teste destinate participanţilor la instruire.

### Realizare curriculă

1. Consultantul împreună cu echipa de implementare a Beneficiarului vor propune și realiza curricula pentru fiecare categorie din grupurile țintă, luând în considerare nevoile de instruire, metodele cele mai potrivite pentru fiecare dintre aceste categorii, disponibilitatea, etc..
2. Ori de câte ori este posibil, se vor utiliza metode de instruire la distanță (e-learning).

#### Rezultate

1. Curricula pentru fiecare categorie din grupurile țintă.

#### Documente generate

1. Documente suport curriculă
2. Plan de instruire
3. Calendarul sesiunilor de instruire

### Realizarea materialelor de instruire pentru formatori și utilizatori

1. Consultantul va pregăti materialele de instruire – manuale, exemple, exerciții, etc. – disponibile în format electronic editabil și manuale ale formatorilor.
2. Consultantul creează infrastructura IT necesară susținerii cursurilor în conformitate cu caietul de sarcini.
3. Consultantul va realiza instruirea formatorilor Beneficiarului, atât pentru diseminarea instruirii utilizatorilor finali, cât și pentru pregătirea acestora în utilizarea materialelor de curs, a metodelor adecvate fiecărui grup țintă și a utilizării metodelor moderne de predare, inclusiv crearea și utilizarea de materiale de instruire folosind e-learning.

#### Rezultate

1. Materiale de instruire pentru formatori și utilizatori (în format letric, cât și electronic)

#### Documente generate

1. Manuale pentru formatori
2. Manuale pentru utilizatori
3. Model de test adecvat fiecărui grup țintă
4. Model Certificat de instruire

### Instruirea formatorilor Beneficiarului (train the trainers)

1. Consultantul va realiza instruirea formatorilor beneficiarului, atât pentru diseminarea instruirii utilizatorilor finali, cât și pentru pregătirea acestora în utilizarea materialelor de curs, a metodelor adecvate fiecărui grup țintă și a utilizării metodelor moderne de predare, inclusiv crearea și utilizarea de materiale de instruire folosind e-learning.
2. Consultantul va instrui 100 de formatori.
3. Consultantul va asigura prezenţa specialistilor din echipa proprie capabili să livreze conţinutul în condiţiile de calitate necesare. Cursurile au ca obiectiv să conducă la obţinerea de deprinderi practice de către formatori, ca atare acestea vor avea, pe lângă module explicative, module cu exerciţii practice, acoperind toate funcţionalităţile sistemului creat şi pus la dispoziţia utilizatorilor finali, în funcţie de natura acestora. În livrarea instruirii, Consultantul va folosi materialele dezvoltate special în acest scop.

#### Rezultate

1. Instruirea formatorilor beneficiarului
2. Grad de promovabilitate de cel puţin 80%

#### Documente generate

1. Tabele de prezenţă
2. Testele de evaluare corectate
3. Certificate de instruire
4. Lista participanţilor care au obţinut un Certificat de instruire
5. Raport recapitulativ al fiecărei sesiuni de instruire

### Instruirea utilizatorilor speciali (administratori de aplicație)

1. Consultantul va realiza instruirea utilizatorilor speciali (administratori de aplicație din aria funcțională), astfel încât aceștia să poată folosi funcționalitățile de administrare ale noului sistem.
2. Consultantul va instrui minim 3 utilizatori speciali (administratori de aplicație) pentru fiecare componentă a noului sistem.

#### Rezultate

1. Instruirea utilizatorilor speciali (administratori de aplicație din aria funcțională)
2. Grad de promovabilitate de cel puţin 80%

#### Documente generate

1. Tabele de prezenţă
2. Testele de evaluare corectate
3. Certificate de instruire
4. Lista participanţilor care au obţinut un Certificat de instruire
5. Raport recapitulativ al ficărei sesiuni de instruire

### Furnizarea de cursuri pentru personalul de specialitate TIC (dezvoltatori, administratori de sistem)

1. Consultantul va face propuneri privind cursurile necesare pentru personalul de specialitate TIC al beneficiarului, astfel încât acesta să poată prelua ulterior sistemul dezvoltat și să-l poată administra și dezvolta. În raport de tehnologiile folosite la dezvoltarea soluției, cursurile standard, procurate de pe piață, vor acoperi domeniile noi pentru dezvoltatorii și administratorii beneficiarului.
2. Cursurile de instruire teoretică și practică vor fi propuse și dimensionate, astfel încât să se asigure acumularea și insușirea temeinică a tuturor tehnologiilor utilizate.
3. Consultantul va instrui minim 20 de persoane de specialitate TIC (dezvoltatori, administratori de sistem), în funcție de infrastructura hardware și software a sistemului eTrezor.

#### Rezultate

1. Furnizarea cursurilor de specialitate necesare pentru personalul de specialitate TIC al beneficiarului (dezvoltatori, administratori de sistem).
2. Grad de promovabilitate de cel puţin 80%

#### Documente generate

1. Tabele de prezenţă cursuri
2. Certificate absolvire curs

# Garanția sistemului

1. Garanţia sistemului eTrezor va fi de 36 luni de la recepția finală.
2. Pentru incidente majore de nefuncționare, cu durata mai mare de 3 ore, indiferent de componentă, garanția sistemului se va prelungi cu un număr de zile corespunzător. În timpul perioadei de garanție, Consultantul va asigura:
   1. întreținere corectivă a sistemului
   2. reparare echipamente conform condițiilor de garanție
   3. accesul la patch-uri și update-uri pentru platformele software
   4. optimizări
   5. actualizare documentații
3. Garanția echipamentelor și a platformelor software va curge de la data livrării acestora.
4. Garanția sistemului va curge de la data acceptanței finale a sistemului.
5. Tabelul de mai jos, prezintă detalierea nivelurilor de gravitate/severitate şi timpii vizaţi pentru răspunsul iniţial (SLA).

|  |  |  |  |
| --- | --- | --- | --- |
| **Nivel de Severitate** | **Descriere** | **Timp de Răspuns iniţial (oferit pe e-mail)1** | **Timp de oferire solutie indirecta 2** |
| Nivel 1 | Impact critic asupra activității:  Problema determină stoparea totală a activităţii. Lucrul nu poate continua, operaţia este esenţială pentru activitate şi situaţia reprezintă o urgenţă. O problemă cu nivel de severitate 1 prezintă una sau mai multe din următoarele caracteristici:   * Corupere date; * O funcţie esenţială nu este disponibilă; * Sistemul se blochează pe perioade nedefinite, determinând întârzieri inacceptabile sau nedefinite pentru resurse şi răspunsuri; * Sistemul se opreşte cu erori şi se opreşte în mod repetat după încercările de a-l reporni | Maxim 2 (două) ore de la semnalarea problemei | Maxim 4 (patru) ore de la semnalarea problemei |
| Nivel 2 | Impact important asupra activității.  Problema determină pierderi importante pentru activitate. Nu este disponibilă nicio soluţie; totuşi operaţiile pot continua în mod limitat. | Maxim 4 (patru) ore de la semnalarea problemei | Maxim 8 (opt) ore de la semnalarea problemei |
| Nivel 3 | Impact mediu asupra activității.  Problema determină pierderi minime pentru activitate. Impactul se manifestă sub forma unui neajuns, care ar putea necesita o soluţionare pentru repunerea în funcţiune | Maxim 1 (o) zi lucrătoare de la semnalarea problemei. | Maxim 2 (doua) zile lucrătoare de la semnalarea problemei. |
| Nivel 4 | Impact minim asupra activității.  Problema nu afectează activitatea. Rezultatul este o eroare minoră, un comportament incorect sau o eroare în documentare, care nu împiedică funcţionarea sistemului. | Maxim 2 (două) zile lucrătoare de la semnalarea problemei | Maxim 5 (cinci) zile lucrătoare de la semnalarea problemei |

1**“Timpul de răspuns iniţial”** reprezintă intervalul de timp maxim cuprins între data recepţionării de către Prestator a solicitarii (pe e-mail) şi trimiterea unui răspuns iniţial pe e-mail către Beneficiar, prin care:

* + Prestatorul confirmă faptul că a luat la cunoştinţă despre problemă;
  + Acceptă nivelul de importanţă propus de Beneficiar (conform unei justificări tehnice şi funcţionale, precum şi conform nivelelor de severitate descrise mai sus);
  + Precizează resursele alocate ce intervin imediat pentru rezolvarea problemei.

2 O soluţie indirectă este un mod de a evita problema sau un mod de a continua operarea în timp ce soluţia efectivă este concepută şi validată. În unele cazuri, o soluţie indirectă poate implica o corecţie a datelor direct pe mediul de productie al Beneficiarului, pentru ca operarea să poată continua, situație în care planul de remediere va trebui aprobat în mod obligatoriu de către Beneficiar. În cazul agreării şi aplicării unei soluţii indirecte, Prestatorul va aplica soluţia finală imediat ce aceasta este disponibilă, într-un interval de timp agreat cu Beneficiarul (astfel încât să se perturbe cât mai puţin activitatea curentă).

# Glosar de termeni și abrevieri utilizate

MF Ministerul Finanţelor

BI sistem de raportare Business Inteligence

ANAF Agenţia Naţională de Administrare Fiscală

AJFP Administrația Județeana a Finanțelor Publice

ATCP Activitatea de Trezorerie și Contabilitate Publică (structura din cadrul AJFP, organizată la nivelul municipiului reședință de judet)

ATCPMB Activitatea de Trezorerie și Contabilitate Publică a Muncipiului București

BNR Banca Naţională a României

COTS Produse de serie ieșite din fabrică

CAB Aplicația Control angajamente bugetare

CIF cod de identificare fiscală

CNIF Centrul Național pentru Informații Financiare

CNP Cod numeric personal

DEDOC Sistemul de Depunere Electronică a Documentelor

DGRFP Direcția Generală Regională a Finanțeor Publice (București, Cluj Napoca, Iași, Galați, Timișoara, Brașov, Craiova, Ploiești)

DGCP Direcția Generală de Contabilitate Publică (structură din cadrul MF)

DGTDP Direcția Generală de Trezorerie și Datorie Publică (structură din cadrul MF)

DW Depozit de date

EP Entitate Publică

Forexebug Sistemul naţional de verificare, monitorizare, raportare şi control al situaţiilor financiare, angajamentelor legale şi bugetelor entităţilor publice

FSE Fondul Social European

IB Internet Banking

ONG Organizații neguvernamentale

ONPCSB Oficiul Național de Prevenire și Combatere a Spălării Banilor

OPT Ordin de plată pentru trezoreria statului (suport de hârtie)

OPTM Ordin de plată pentru trezoreria statului multiplu (suport de hârtie)

OPME Ordin de plată multiplu electronic

PF / PFA Persoana fizică (autorizată)

PUA Punctul Unic de Acces

ReGis Sistem electronic de decontare pe bază brută în timp real care asigură schimbul de instrucţiuni de plată între participanţi şi decontarea finală (definitivă) a transferurilor de fonduri aferente acestora în mod continuu, tranzacţie cu tranzacţie, precum şi decontarea finală (definitivă) a poziţiilor nete provenite de la sistemele cu decontare pe bază netă şi a transferurilor de fonduri aferente operaţiunilor cu instrumente financiare.

SENT Sistem electronic de compensare multilaterală a plăţilor, care asigură schimbul de instrucţiuni de plată între participanţii la sistem, conversia instrucţiunilor de plată de tip transfer credit în formatul utilizat de participantul destinatar, calculează poziţiile nete şi net-nete ale participanţilor prin compensare multilaterală şi iniţiază decontarea instrucţiunilor de decontare pe bază netă sau net-netă în sistemul ReGIS pentru instrucţiunile de plată denominate în lei.

SDIRSIP Serviciul Decontări Intertrezorerii și Relații cu Sistemul Interbancar de Plăți (structura din cadrul DGCP, în cadrul careia funcționează Trezoreria Centrală)

SDONPE Serviciul Decontări, Operaţiuni cu Numerar şi Produse Electronice (structura din cadrul AJFP – ATCP, organizată la nivelul municipiului reședință de judet)

SEP Sistemul Electronic de Plăţi

SNM Platforma electronică de Notificări şi Mesagerie

SASNRF Serviciul Administrarea Sistemului National de Raportare ForExe (structură din cadrul DGCP)

SPI Serviciul Plăți Interbancare (structura din cadrul DGTDP)

TOC Trezoreria Operativă Centrală (structura din cadrul DGCP)

TS Trezoreria Statului

UAT Unități administrativ teritoriale

UTTS Unitate teritorială a Trezoreriei Statului