

Caiet de sarcini
„Portalul IMM-urilor din România”

Ministerul Comunicațiilor și Societății Informaționale

Conținut

1	OBIECTIVELE PROIECTULUI	4
1.1	Obiective pe termen scurt	5
1.2	Obiective pe termen lung	5
1.3	Beneficii și beneficiari	7
2	CERINȚE PRIVIND SOLUȚIA TEHNICĂ	9
2.1	Cerințe generale	9
2.2	Prevederi generale de securitate	10
3	DESCRIEREA TEHNICĂ A PROIECTULUI	12
3.1	Caracteristici generale	12
3.2	Arhitectura funcțională a sistemului	15
3.3	Cerinte privind serviciile de implementare a sistemului	20
3.3.1	Activitati	20
3.3.2	Volumetrie servicii de dezvoltare	21
3.4	Componente de baza ale Sistemului	23
3.4.1	Modul Portal	23
3.4.2	Modul de Management al Documentelor	43
3.4.3	Sistem de Baze de Date Relationale	49
3.4.4	Platforma de Integrare a Componentelor	53
3.4.5	Platforma de Analiza si Raportare cu Suport de Harta	56
3.5	Componente de suport ale Sistemului	68
3.5.1	Virtualizarea resurselor de procesare	68
3.5.2	Confidențialitatea datelor	70
3.5.3	Autentificare tip OTP	73
3.5.4	Optimizare si control a accesului la servicii	78
3.5.5	Monitorizare acces la componentele sistemului	83
3.5.6	Autentificare pe baza recunoasterii semnăturii olografe	87
3.5.7	Salvare si restaurare date	89
3.6	Infrastructura hardware	93
3.6.1	Echipamente tip server	93

3.6.2	Alte echipamente	105
4	CERINTE PRIVIND SERVICIILE DE PROMOVARE SI PUBLICITATE	116
4.1	Plan de informare și publicitate	116
4.2	Organizare evenimente de promovare a proiectului	116
4.3	Editarea, producția, tipărirea/multiplicarea, inscripționarea și distribuția de materiale promoționale.....	118
4.4	Elaborare comunicate de presa.....	119
4.5	Realizare pagina Web si publicare anunturi.....	119
5	CERINTE PRIVIND SERVICIILE DE MANAGEMENT DE PROIECT	121
6	RESURSE	125
6.1	Personal și instruire	125
6.1.1	Managementul proiectului, personal si instruire.....	125
6.2	Resurse materiale	138
7	MENTENANTA SI SUSTENABILITATE	140
7.1	Mentenanță	140
7.2	Sustenabilitate	144

1 OBIECTIVELE PROIECTULUI

Răspândirea largă a tehnologiilor informatice și comunicațiilor din zilele noastre, are ca rezultat piețe competitive. Companiile de toate mărimile trebuie să facă față unui mediu de business în continuă schimbare, unde vechile bariere nu mai există, fiind înlocuite de competiția privind produsele și prețurile. De aceea mult mai multe companii încearcă să răspundă provocărilor concentrându-se pe competențele lor de bază și să coopereze cu alte companii pentru a-și completa lanțul de valori.

Totuși, înainte și în timpul cooperării, companiile trebuie să-și coordoneze activitățile.

Aceste procese de coordonare sunt generatoare de cost, care ar trebui minimizate pentru a maximiza beneficiul cooperării.

Aceste costuri trebuie minimizate mai ales în cazul companiilor de dimensiuni mici și medii, datorită resurselor financiare restrânse.

Mai mult decât atât tehnologia induce o competiție globală, în care factorul timp devine un factor critic de succes, obligând astfel companiile să reacționeze rapid la noile oportunități de business.

Prin urmare capacitatea de a fi pregătit pentru o nouă inițiativă sau de a se alătura unui business nou, devine un task obligatoriu al management-ului. Aceasta abilitate reprezintă elementul constitutiv al noțiunii de „interoperabilitate”, definită ca fiind “capacitatea a doua sau mai multe sisteme sau componente să schimbe informații și să utilizeze această informație”.

Interoperabilitatea este definită ca fiind o proprietate a unui sistem tehnic, fiind privită strict ca un fenomen tehnologic.

Obiectivul acestui proiect constă în dezvoltarea interoperabilității bazelor de date destinate IMM-urilor.

Din punct de vedere tehnic, principala condiție pentru a permite interoperabilitatea o reprezintă posibilitatea de a schimba date prin intermediul unui “gateway” ce permite stabilirea unor interacțiuni .

Aceasta conduce la concluzia; interoperabilitatea, din acest punct de vedere constituie doar o proprietate a unui sistem.

Totuși interoperabilitatea companiilor nu reprezintă doar un sistem tehnic, fiind un sistem organizațional complex.

Întreprinderile mici și mijlocii nu pot fi vizualizate doar ca obiect sistem, ci și ca un sistem strategic, social.

De aceea noțiunea de interoperabilitatea între întreprinderile mici și mijlocii nu trebuie percepută doar la nivel tehnic, ci și semantic, la nivelul aplicațiilor și al proceselor.

1.1 Obiective pe termen scurt

Strategia Ministerului Comunicațiilor și Societății Informaționale referitoare la informatizarea serviciilor publice la nivel central și local trebuie să urmărească cu precădere câteva direcții de acțiune:

- Creșterea eficienței aparatului administrativ prin folosirea noilor tehnologii electronice de comunicare;
- Orientarea serviciilor publice spre necesitățile cetățenilor și ale oamenilor de afaceri;
- Asigurarea accesului liber la informațiile publice;
- Transparența în exercitarea actului administrativ;
- Îndeplinirea standardelor administrației europene, în vederea interconectării cu sistemele statelor din Uniunea Europeană;

În acest sens se dorește să se pună la dispoziția Administrației Centrale o structură de tip portal electronic care să ofere posibilitatea de a integra eventualele aplicații existente ale instituției și pe care Administrația Centrală să o utilizeze în scopul publicării de conținut digital, pentru interacțiunea cu cetățenii și mediul de afaceri.

1.2 Obiective pe termen lung

Informatizarea administrației publice este parte integrantă a “Strategiei naționale pentru promovarea noii economii și implementarea societății informaționale”, așa cum este ea reglementată în legislația românească. Modelul ce se dorește a fi implementat este acela al unei administrații publice orientate spre deservirea cetățenilor, al unei administrații care să susțină un schimb intensiv de informații și date, atât în interiorul sistemului între instituțiile publice, cât și în relația cu exteriorul, cu mediul de afaceri și organizațiile neguvernamentale.

Informatizarea administrației publice se înscrie într-o suită de măsuri guvernamentale ce vizează reformarea acestui sector de activitate din România. Strategia guvernamentală de informatizare a administrației publice urmărește atingerea indicatorilor stabiliți de către Consiliul European, definiți în anul 2002, sub conceptul de “procentaj al serviciilor publice de baza disponibile on-line”, și redefiniți în 2005, ca “număr al serviciilor publice de baza disponibile integral on-line”.

Printre obiectivele globale ale informatizării administrației publice din România regăsim următoarele:

- Îmbunătățirea calității serviciilor publice având ca beneficiari cetățenii și agenții economici;
- Accesul cetățenilor la informația de interes public va fi astfel asigurat evitându-se restricționările legate de spațiu și timp. Totodată, soluțiile de securitate implementate la nivelul instituțiilor publice vor asigura deplină confidențialitate și integritate a datelor și informațiilor transmise sistemului. Îndeplinirea unor criterii de excelență și calitate la nivelul instituțiilor publice va contribui decisiv la formarea unei imagini profesioniste a organizațiilor în rândul celor cu care acestea interacționează.
- Modernizarea administrației publice;
- Electronizarea instituțiilor publice se înscrie în tendința generală de a aduce administrația publică românească la standardele europene.
- Dezvoltarea sectorului IT&C, prin lansarea de noi proiecte și implementarea de noi sisteme informatice integrate la nivelul instituțiilor publice.
- Pentru punerea în aplicare a strategiei guvernamentale referitoare la reformarea administrației prin informatizare, este necesară derularea de proiecte specifice tehnologiilor informației și comunicațiilor. Pentru implementarea unor astfel de proiecte, sectorul privat este stimulat să proiecteze și să realizeze sisteme competitive, integrate. Succesul acestor proiecte va aduce companiilor private IT&C recunoaștere și performanțe financiare importante, consolidându-le poziția în piață.
- Creșterea calității vieții cetățenilor prin utilizarea noilor tehnologii
- Prin promovarea la nivelul administrației publice a tehnologiilor informatice competitive, orientate spre Internet, se va asigura o creștere a satisfacției cetățenilor în ceea ce privește relația cu instituțiile statului. Toate aceste acțiuni vor putea fi derulate în spațiul virtual pe care Internetul îl oferă, în condiții de maximă siguranță și confidențialitate, fără alte limitări temporale, exceptându-le pe cele legale.

- Menținerea și dezvoltarea unei capacități de cercetare-dezvoltare-inovare susținută de un transfer tehnologic activ către producătorii de bunuri și servicii.
- Ținând cont de dinamica instituțională, de liberă concurență din spațiul european precum și de noile principii ce vor governa conducerea instituțiilor publice, furnizorii de soluții informatice în domeniul serviciilor publice, vor trebui să mențină un ritm alert de cercetare și dezvoltare pentru a putea veni în întâmpinarea solicitărilor pieței cu produse și servicii competitive, care să mențină și să crească calitatea serviciilor publice. Furnizarea de servicii complete între unități ale administrației publice centrale și locale, diferite, implică îndeplinirea interoperabilității totale a sistemelor informaționale centrale cu cele ale administrațiilor publice locale, care sunt desemnate din ce în ce mai mult să asigure coordonarea directă a serviciilor furnizate către cetățeni sau agenți economici, devenind astfel interfața administrației publice centrale.

1.3 Beneficii și beneficiari

Întreprinderile mici și mijlocii, ca forme specifice de organizare a activității economice, sunt direct implicate în procesul de transformare impus mediului socio-economic de explozia tehnologica a ultimului deceniu.

Explozia Internet-ului, dezvoltarea comerțului electronic conduc la transformarea IMM-urilor clasice în organizații pentru care sistemul informatic nu mai reprezintă un element complementar, ci chiar fundamentul structurii organizaționale.

Realizarea unei infrastructuri privind interoperabilitatea între întreprinderile mici și mijlocii s-ar concretiza în următoarele beneficii:

- Noile servicii electronice vor deveni disponibile tuturor utilizatorilor, deoarece va exista infrastructura corespunzătoare, deployment-ul va fi centralizat, iar integrarea va urmări standarde europene
- Fiecare utilizator va avea o identitate unica fata de toate serviciile, datorită autentificării securizate
- Costurile pentru IMM-uri și Administrația Centrală vor fi reduse datorită:
 - infrastructurii comune

- scăderea timpilor de procesare
- eliminarea redundantei
- vor fi garantate calitatea și securitatea serviciilor oferite

Sistemul va asigura accesul cetățenilor și agențiilor economice la două tipuri de informații:

- publică – date generale despre materiale și acte normative de interes public, despre orar, funcționare, competențele comisiilor din structurile administrațiilor publice
- privată – aplicația dedicată îi oferă posibilitatea creării unei legături directe și securizate cu administrația publică, în care datele de acces personale folosite sau solicitate sunt protejate;

Cetățenii și agenții economici vor putea obține informațiile necesare fără a se mai deplasa la sediul instituțiilor publice, și fără a mai consuma din timpul alocat altor activități.

2 CERINȚE PRIVIND SOLUȚIA TEHNICĂ

2.1 Cerințe generale

Proiectul „Portalul IMM-urilor din România” urmărește creșterea calității serviciilor publice oferite către cetățeni și mediul de afaceri. Astfel, ne propunem ca prin acest proiect să oferim posibilitatea autorităților locale și centrale de a livra serviciile publice și prin intermediul mijloacelor electronice, și de a livra anumite servicii publice în mod organizat, fără ca beneficiarii acestor servicii să se deplaseze la sediile acestora. Mai mult decât atât, ne propunem să oferim instrumente puternice de informare pentru beneficiarii finali – cetățenii în vederea informării mai eficiente a acestora dar și a creșterii transparenței instituțiilor publice.

În acest sens, vom pune la dispoziția atât a cetățenilor, cât și a autorităților centrale și locale o platformă software cu ajutorul căreia beneficiarii finali să poată accesa prin intermediul unei conexiuni la Internet o parte din serviciile oferite de către autorități.

În cadrul proiectului se va acorda o importanță deosebită :

- Orientării pe valoarea adăugată a serviciilor electronice (centrarea pe nevoile cetățeanului/mediului de afaceri) – orice serviciu furnizat de o instituție publică trebuie să satisfacă o nevoie a utilizatorului, persoana fizică sau juridică ;
- Crearea premiselor pentru realizarea accesului centralizat - serviciile publice vor fi furnizate printr-un portal electronic cu posibilitatea de a fi integrate într-un punct unic de acces centralizat la nivelul mai multor instituții publice;
- Accesibilitate și transparența – informațiile, procesele și serviciile electronice furnizate de către administrația publică trebuie să fie accesibile și transparente tuturor categoriilor de beneficiari, inclusiv grupurilor dezavantajate, într-o formă inteligibilă pentru aceștia, atât prin mijloace tradiționale, cât și prin mijloace electronice ;
- Corectitudinea și autenticitatea informațiilor – corectitudinea și autenticitatea informațiilor oferite prin intermediul portalului “Interoperabilitate Întreprinderi Mici și Mijlocii” sunt garantate de către instituția publică care generează și gestionează acele informații ;

- Reutilizare și eficiența – implementarea și dezvoltarea serviciilor electronice trebuie să se realizeze într-un mod coordonat și integrat, promovând reutilizarea soluțiilor/sistemelor și a informațiilor/datelor la nivelul administrației publice în scopul eliminării redundanței informațiilor solicitate cetățenilor/mediului de afaceri ;
- Securitate și confidențialitate – serviciile electronice trebuie să respecte și să protejeze identitatea electronică a persoanelor, să respecte dreptul persoanelor la confidențialitatea datelor personale și să prevină orice atac informatic asupra acestora ;
- Standardizarea și interoperabilitatea – se vor utiliza tehnologii, standarde și arhitecturi deschise, scalabile și flexibile, în vederea asigurării interoperabilității atât la nivel național cât și european .

În afara acestor cerințe generale, se vor respecta și cerințele detaliate cuprinse în prezentul document în descrierea componentelor de bază ale proiectului în cadrul capitolului 3.3 – „Componente de bază ale Sistemului”.

2.2 Prevederi generale de securitate

Proiectul va respecta următoarele prevederi generale de securitate:

- Toate aplicațiile, componentele, paginile și serviciile web vor fi protejate împotriva tuturor tipurilor de atacuri informatice cunoscute;
- Este interzisă preluarea de date sau informații, sub formă direct sau indirect executabilă, prin intermediul mijloacelor de preluare de date sau informații de la utilizatori;
- Este interzisă transmiterea, sub orice formă, de date sau cod direct sau indirect executabile, între aplicații, componente, pagini sau servicii web;
- Este interzisă transmiterea în clar a informațiilor între aplicații, componente, pagini sau servicii web; este permisă transmiterea între aplicații, componente, pagini sau servicii web a informațiilor numai în formă criptată, folosind algoritmi de criptare publici, standardizați, cu minim următoarele caracteristici:

- algoritmi cu cheie simetrică de criptare;
- lungimea cheii de criptare minim 1024 biți;
- Este interzisă transmiterea în rețea (sau Internet) sau stocarea în bazele de date în clar a informațiilor de identificare/autentificare sau a mijloacelor de recuperare a datelor de autentificare ale utilizatorilor, sau a informațiilor care pot reprezenta informații confidențiale sau secrete; este permisă transmiterea în rețea (sau Internet), respectiv stocarea în bazele de date a astfel de informații numai în formă criptată, folosind algoritmi de criptare publici, standardizați, cu minim următoarele caracteristici:
 - algoritmi cu cheie simetrică de criptare;
 - lungimea cheii de criptare minim 1024 biți;
- Este interzisă posibilitatea referirii directe a unei resurse prin Internet (aplicație, componentă, pagina sau serviciu web, document), altfel decât urmând și respectând fluxurile normale și corecte ale aplicațiilor, componentelor, paginilor sau serviciilor web; excepție fac documentele sau informațiile pentru care utilizatorul și-a dat acordul explicit pentru facilitarea accesării din Internet;
- Documentele stocate, conform fluxurilor normale, corecte ale aplicațiilor, componentelor, paginilor sau serviciilor web, vor fi stocate în clar și vor avea nume de fișier unic generate; accesibile direct din Internet vor fi numai documentele pentru care utilizatorul și-a dat acordul explicit pentru facilitarea accesării din Internet;
- Aplicațiile vor realiza log-uri detaliate cu toate operațiunile realizate efectuate ulterior autentificării.

Se vor respecta și prevederile specifice de securitate prin intermediul componentelor dedicate – din cadrul componentelor de suport ale Sistemului (a se vedea capitolul 3.8 – „Componente de suport ale Sistemului” din prezentul document).

3 DESCRIEREA TEHNICA A PROIECTULUI

3.1 Caracteristici generale

Proiectul urmărește creșterea calității serviciilor publice oferite către cetățeni, mediul de afaceri. Astfel, prin acest proiect vom oferi posibilitatea autorităților locale și centrale de a livra serviciile publice și de a informa utilizatorii și prin intermediul mijloacelor electronice, și de a livra anumite servicii publice în mod organizat, fără ca beneficiarii acestor servicii să se deplaseze la sediile acestora sau să apeleze în mod obligatoriu la mijloace alternative de comunicare, de tipul e-mail sau telefon către serviciul de relații cu publicul. Mai mult decât atât, ne propunem să oferim instrumente puternice de informare pentru beneficiarii finali – cetățenii în vederea informării mai eficiente a acestora dar și a creșterii transparenței instituțiilor publice.

În acest sens, vom pune la dispoziția Administrației Centrale o platforma software cu ajutorul căreia beneficiarii finali să poată accesa prin intermediul unei conexiuni la Internet informațiile oferite de către acesta.

În cadrul proiectului se va acorda o importanță deosebită orientării pe valoarea adăugată a serviciilor electronice (centrarea pe nevoile cetățeanului/mediului de afaceri) – orice serviciu furnizat de administrația publică trebuie să satisfacă o nevoie a utilizatorului, persoana fizică sau juridică;

Segregarea atribuțiilor – Ministerul va pune la dispoziție și va administra din punct de vedere tehnic platforma software pentru Administrația Centrală, acesteia revenindu-și atribuțiile de management al conținutului informatic publicat pentru cetățeni și mediul de afaceri;

Asigurarea premiselor de integrare a sistemului de interacțiune cu utilizatorii cu alte soluții similare – care vor deservi diferite instituții publice – soluții construite cu același scop și anume cel de a livra către grupurile țintă servicii publice online;

Accesibilitate și transparența – informațiile, procesele și serviciile electronice furnizate de către administrația publică trebuie să fie accesibile și transparente tuturor categoriilor de beneficiari, inclusiv grupurilor dezavantajate, într-o forma inteligibilă pentru aceștia, atât prin mijloace tradiționale, cât și prin mijloace electronice;

Corectitudinea și autenticitatea informațiilor – corectitudinea și autenticitatea informațiilor oferite prin intermediul portalului „Interoperabilitate Întreprinderi Mici și Mijlocii” sunt garantate de către instituția publică care generează și gestionează acele informații;

Reutilizare și eficiență – implementarea și dezvoltarea serviciilor electronice trebuie să se realizeze într-un mod coordonat și integrat, promovând reutilizarea soluțiilor/sistemelor și a informațiilor/datelor la nivelul administrației publice în scopul eliminării redundantei informațiilor solicitate cetățenilor/mediului de afaceri;

Securitate și confidențialitate – serviciile electronice trebuie să respecte și să protejeze identitatea electronică a persoanelor, să respecte dreptul persoanelor la confidențialitatea datelor personale și să prevină orice atac informatic asupra acestora;

Standardizarea și interoperabilitatea – se vor utiliza tehnologii, standarde și arhitecturi deschise, scalabile și flexibile, în vederea asigurării interoperabilității atât la nivel național cât și european;

Întreprinderile mici și mijlocii (IMM) sunt puternic influențate de provocările globale și de modificările condițiilor de business. Fiecare IMM trebuie să fie datorită dimensiunii ei și consecvent datorită deschiderii; mult mai dinamică decât întreprinderile mari.

Întreprinderile mici și mijlocii nu au suficiente resurse pentru a-și actualiza sau dezvolta propriile programe software. Având în vedere aceste condiții, condițiile necesare succesului constau în reutilizarea sistemelor software.

Sistemele software ce sunt utilizate de IMM-uri trebuie să suporte dinamica business-ului modern. Prin urmare, un astfel de sistem software trebuie să fie deschis și dinamic modificabil. O soluție clasică o reprezintă dezvoltarea rapidă a unui nou software sau actualizări ale celui existent. Complexitatea în continuă creștere a sistemelor software determină ca o astfel de soluție să fie din ce în ce mai puțin fezabilă.

Această problemă devine foarte serioasă pentru IMM-uri din următoarele motive:

- IMM-urile nu au resurse suficiente și experți IT pentru a dezvolta repetat de la zero sisteme software care să cuprindă noile schimbări.
- Devine uneori foarte dificil pentru angajații IMM să utilizeze sistemele în continua modificare.
- Deasemenea este dificil și pentru IMM să dezvolte un proces de business sigur și stabil. IMM-urile nu au suficiente date de business pentru a proiecta procese repetabile sau chiar optimizate. Procesele de business sunt aproape întotdeauna schimbate din mers datorită modificărilor externe de business.
- IMM-urile au posibilitate limitată de a aplica standarde de software complexe cum ar fi (IEEE – Institute of Electrical and Electronics Engineers, ISO-International

Organization for Standardization, W3C-World Wide Web Consortium sau OASIS-Organization for the Advancement of Structured Information Standards). Complexitatea standardelor poate fi un motiv substanțial pentru scăderea interesului în noile dezvoltări SOA (Service – oriented architecture).

Singura soluție fezabilă o constituie reutilizarea sistemelor actuale, integrarea lor împreună și cu sisteme third-party obținerea de sisteme performante noi.

Orientarea către servicii (SO – service orientation) și arhitectura SO (SOA) oferă un mediu de lucru pentru a realiza aceasta.

Arhitectura orientate servicii deține o rețea de bază de servicii care se cunosc între ele. În IMM baza o constituie un număr mic de servicii absolut independente. IMM utilizează adesea tehnici folosite în SOA dar exista o rețineră în aplicarea standardelor ridicate SOA în forma suportata de furnizorii mari de software.

Sistem SOA pentru IMM

Problemele punctate mai sus pot fi rezolvate prin integrarea aplicațiilor cum ar fi sistemele realizate având arhitectura orientate servicii cu următoarele proprietăți:

- SOA să incorporeze sistemele vechi, sisteme third-party și eventual sisteme nou dezvoltate, astfel încât să se comporte la fel ca în lumea reala a serviciilor; tehnic pot fi perechi ale unei rețea virtuale peer-to-peer .

Layer-ul de transformare de conversie a unei astfel de rețele se poate baza pe diferite instrumente sau medii de lucru ; Enterprise Service Bus, www sau alte medii de transport. Aceste instrumente se pot combina.

Dezvoltarea și utilizarea sistemelor software în IMM suferă de lipsa datelor și a informațiilor, de lipsa experților în acest domeniu, resurse limitate, deficiente în procesul de management. Soluția poate fi software având o varianta specifică de SOA. Sistemele cu SOA sunt rețele virtuale peer-to-peer, unde fiecare nod din rețea reprezintă componente software autonome ce implementează permanent procese active numite servicii.

Ca noduri într-o rețea peer-to-peer , serviciile trebuie să fie capabile să comunice în mod asincron. Comunicațiile sincrone sunt deasemenea posibile dar de obicei nu sunt preferate sau nu sunt aplicabile. Soluția poate fi bazată SOA pe o generalizare, suportând reutilizarea sistemelor vechi și produse third-party.

Integrarea sistemelor vechi și a aplicațiilor într-o arhitectura orientate servicii.

Colaborarea între sistemele partenerilor de business pot fi similare cu serviciile din sistemul propriu. Aceasta are multe avantaje tehnice la fel și avantaje organizaționale, deoarece simplifică în, out, și colaborarea cu parteneri, în general. Singura modalitate cunoscută de implementare facilă este proiectarea unui sistem având o arhitectura orientate servicii, adică un o rețea virtuala de sisteme peer-to-peer unde sistemele (nodurile) sunt sisteme vechi incorporate, produse third-party și chiar și sisteme informaționale ale componentelor organizaționale.

Nodurile din rețea colaborează prin intermediul mesajelor. Mesajul trebuie să aibă un format care să fie bine înțeles de către utilizatori. În cazul sistemelor SOAP , aceasta înseamnă că mesajele trebuie să fie codate SOAP. Cu alte cuvinte kernel-ul soluției este un sistem orientat servicii cu servicii ce au interfață utilizabila.

3.2 Arhitectura funcțională a sistemului

Din punct de vedere funcțional arhitectura sistemului include următoarele componente de baza (aceste componente sunt descrise în cadrul capitolului 3.3 – „Componente de baza ale Sistemului” din prezentul document):

- Modul Portal;
- Modulul de Management al Documentelor;
- Sistem de Baze de Date Relationale;
- Platforma de Integrare a Componentelor;
- Platforma de Analiza și Raportare cu Suport de Harta.

Totodata, arhitectura sistemului include și componente dedicate de suport (aceste componente sunt descrise în cadrul capitolului 3.4 – „Componente de suport ale Sistemului” din prezentul document):

- Virtualizarea resurselor de procesare;
- Confidentialitate datelor;
- Autentificarea tip OTP;
- Optimizare și control a accesului la servicii;

- Monitorizare acces la componentele sistemului;
- Autentificare pe baza recunoașterii semnăturii olografe;
- Salvare și restaurare date.

Portalul „Interoperabilitate Întreprinderi Mici și Mijlocii„ trebuie să ofere următoarele funcționalități generale:

- interfață web, facilă pentru prezentare și navigare rapidă și simplă
- posibilitatea de a personaliza conținutul
- caracteristici pentru securitate ridicată
- să fie un sistem deschis bazat pe standardele existente în domeniu
- să permită administrare ușoară
- dezvoltarea aplicațiilor să se facă ușor, respectând standardele în domeniu
- să fie un sistem scalabil care să funcționeze în arhitecturi cu disponibilitate ridicată
- portalul trebuie să ofere un punct centralizat de lucru pentru utilizatori și o interfață unitară către alte sisteme informatice

Platforma portal trebuie să conțină cel puțin următoarele componente, fără a fi nevoie de achiziționarea de licențe suplimentare:

- server de aplicație;
- modulul de management al documentelor;
- server HTTP;
- sistem de gestiune al bazelor de date relaționale;
- director LDAP;
- componentă pentru dezvoltare aplicații și extindere funcționalități în portal;
- componentă pentru managementul utilizatorilor și accesul la sistem;

- componenta de formulare electronice;
- componenta de mesagerie instantanee;
- motor de flux (workflow engine).

In continuare se va prezenta arhitectura functionala a modului Portal, ca si componenta de integrare a restului de componente ale sistemului.

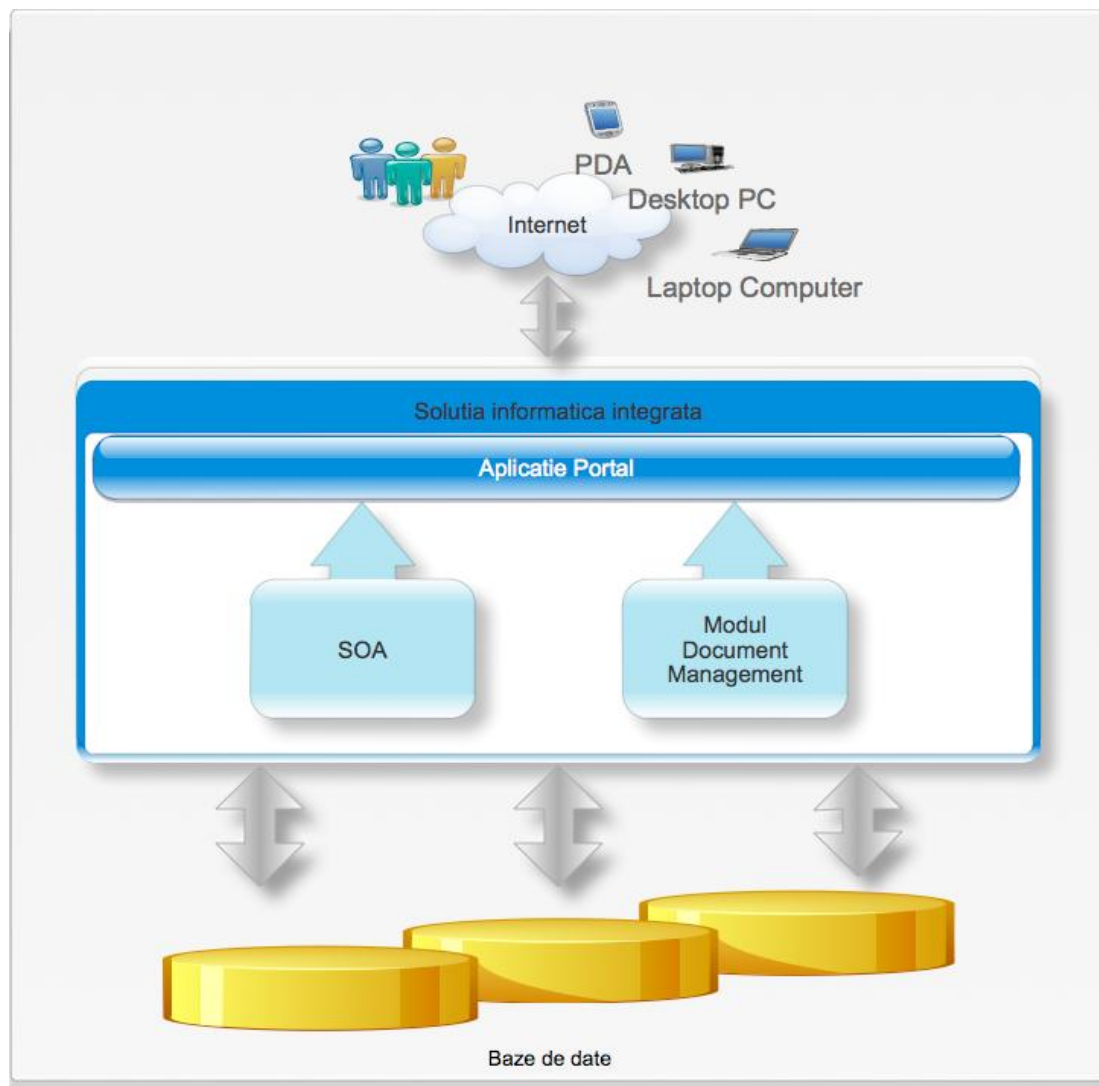


Figura 1: Arhitectura funcțională a soluției de interacțiune cu cetățenii și mediul de afaceri

Soluția conceptuală propusă trebuie să aibă asigurat suportul hardware și de comunicații corespunzător. În acest sens, arhitectura hardware și de comunicații ce trebuie asigurată trebuie să fie de natură să sigure disponibilitatea maximă a soluțiilor software instalate.

Platforma portal:

- trebuie să poată fi implementată pe următoarele platforme sistem de operare: Microsoft Windows Server 2003, Microsoft Windows 2008, Linux (SUSE, RHEL), Solaris SPARC, Solaris x64.
- trebuie să permită implementarea atât pe sisteme de operare pe x32 cât și x64.
- Să suporte următoarele platforme de baze date: Oracle, IBM DB2, MS SQL Server.
- Să se integreze cu diferite sisteme LDAP cum ar fi: MS Active Directory, Tivoli Directory Server, Novel eDirectory, Sun Java System Directory Server.

Pentru o mai bună gestiune a resurselor hardware, este necesar ca sistemele să ofere suport pentru virtualizare sau partiționare logică sau fizică a resurselor interne: procesoare, memorie, dispozitive de intrare/ieșire. În acest fel este asigurată posibilitatea de mapare facilă a resurselor de procesare către aplicațiile care au un grad de solicitare mai mare la un moment dat.

Este necesar ca sistemele pe care vor rula aplicațiile să aibă instalate resurse suficiente pentru procesare și stocare în termeni de: procesoare, memorie internă, unități de stocare internă etc.

Modelul arhitectural este prezentat în figura următoare:

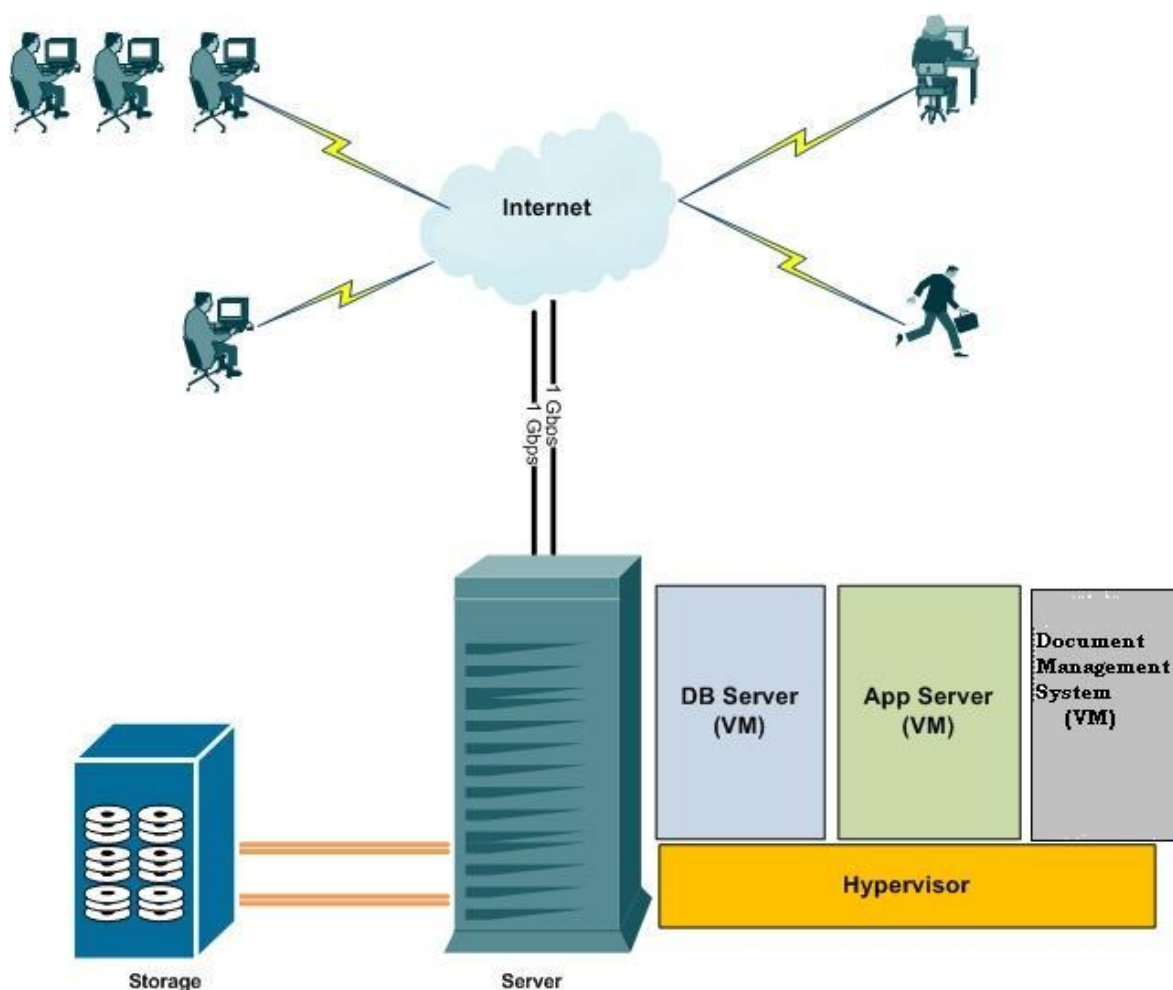


Figura 2: Arhitectura hardware a soluției de interacțiune cu cetățenii și mediul de afaceri

Arhitectura propusă este bazată pe tehnologia Internet și este compusă din trei nivele: Client, Aplicație și Baza de Date.

Nivelul Client – este reprezentat la rândul lui din 2 subnivele: Nivelul utilizatori și Nivelul prezentare

- **Nivelul utilizatori** – este reprezentat de stațiile de lucru ale utilizatorilor interni și externi. De pe stațiile de lucru, folosind un browser web, utilizatorii vor interacționa cu portalul de acces.
- **Nivelul prezentare** – este compus din server web care rulează serviciile de prezentare și acces pentru utilizatorii externi.

Nivelul Aplicație – este compus din următoarele funcții:

- Server Portal Web - pe rulează serviciile portalului.

- Server de aplicație - pentru soluția de integrare a aplicației cu sistemele existente.

Nivelul Baza de Date :

- Serverele de baze de date vor fi conectate la un Storage Area Network (SAN).

3.3 Cerinte privind serviciile de implementare a sistemului

3.3.1 Activitati

Implementarea (din punct de vedere tehnic a) sistemului vizeaza urmatoarele activitati distincte:

Numar Activitate	Denumire activitate proiect
1	Livrarea catre Beneficiar a echipamentelor hardware de suport a sistemului: <ul style="list-style-type: none"> • Instalarea infrastructurii hardware de suport a sistemului: <ul style="list-style-type: none"> ○ Punerea in functiune, configurarea si testarea echipamentelor; ○ Testarea integrata, acolo unde e cazul, a functionalitatii echipamentelor.
2	Livrarea catre Beneficiar a licentelor software aferente componentelor sistemului, atat cele de baza cat si cele de suport: <ul style="list-style-type: none"> • Instalarea a infrastructurii software a sistemului: <ul style="list-style-type: none"> ○ Instalarea si configurare componente; ○ Testarea componentelor.
3	Dezvoltarea sistemului, in cadrul componentelor software: <ul style="list-style-type: none"> • Analiza si proiectare: <ul style="list-style-type: none"> ○ Analiza (tinand cont de complexitatea activitatilor specifice beneficiarului si a calendarului incarcat al utilizatorilor acestuia implicati in etapa de analiza, ofertantii vor lua in calcul privind propriul efort un numar minim de 70 de zile-om pentru aceasta etapa); ○ Proiectare; ○ Elaborare specificatii de dezvoltare. • Instalare, configurare si dezvoltare in cadrul componentelor software: <ul style="list-style-type: none"> ○ Dezvoltare in cadrul componentelor software; ○ Integrarea componentelor in cadrul sistemului; ○ Deployment; ○ Documentare. • Testare functionala si integrata (tinand cont de complexitatea activitatilor specifice beneficiarului si a calendarului incarcat al utilizatorilor acestuia implicati in etapa de analiza, ofertantii vor lua in calcul privind propriul efort un numar minim de 60 de zile-om pentru aceasta etapa):

	<ul style="list-style-type: none"> ○ Integrarea sistemului cu aplicatiile/sistemele cu care acesta trebuie sa se integreze (lista completa a acestora se va definitiva in perioada de analiza aferenta implementarii sistemului); ○ Testare integrata; ○ Acceptanta.
4	<p>Servicii de populare cu date a bazelor de date ale sistemului, care se constituie din preluarea (tinand cont de complexitatea activitatilor specifice beneficiarului si a calendarului incarcat al utilizatorilor acestuia implicati in etapa de analiza, ofertantii vor lua in calcul privind propriul efort un numar minim de 15 de zile-om pentru aceasta etapa):</p> <ul style="list-style-type: none"> • datelor necesare din diverse aplicatii/baze de date (lista completa a acestora se va definitiva in perioada de analiza aferenta implementarii sistemului); • altor date necesare lansarii in folosinta a sistemului.
5	<p>Servicii de dezvoltare de continut electronic:</p> <ul style="list-style-type: none"> • pentru modulul de Portal.
6	<p>Instruire a utilizatorilor sistemului, care include (tinand cont de complexitatea activitatilor specifice beneficiarului si a calendarului incarcat al utilizatorilor acestuia implicati in etapa de analiza, ofertantii vor lua in calcul privind propriul efort un numar minim de 20 de zile-om pentru aceasta etapa):</p> <ul style="list-style-type: none"> • Instruirea in clasa a utilizatorilor desemnati de Beneficiar cu ajutorul unui instructor; • Livrarea catre Beneficiar a materialelor aferente instruirii in clasa pe suport electronic.
7	<p>Servicii de suport, care includ:</p> <ul style="list-style-type: none"> • Suport acordat Beneficiarului in perioada de Go-Live a proiectului.
8	Garantie

3.3.2 Volumetrie servicii de dezvoltare

In perioada de analiza aferenta implementarii sistemului informatic sunt incluse minim urmatoarele:

- Elaborarea documentelor de arhitectura functionala detaliata a sistemului (stabilire in detaliu a componentelor si sub-componentelor de lucru);
- Stabilirea fluxurilor informationale intre componente/sub-componentele sistemului;
- Elaborare identitate vizuala pentru Portal;
- Definire zone portal, niveluri de acces asociate, profiluri utilizator si tipuri de informatii asociate;
- Definire tipuri de date, structuri de date, metadate;

- Definirea schemelor de securitate (nivele de acces, roluri, etc.);
- Definire specificatii complete privind documentele vehiculate in cadrul portalului;
- Definire si elaborare nomenclatoare de lucru (aproximativ 140 de nomenclatoare lucru);
- Elaborare detaliata a specificatiilor privind serviciile oferite prin intermediul Portalului (aproximativ 40 de servicii);
- Definirea fluxurilor de lucru necesare (aproximativ 30 de fluxuri de lucru, cu o medie de 4-8 pasi si 3-5 actori; atasare perioade de rezolutie, caracteristici de delegare, etc.);
- Elaborare interfete de lucru (vizualizare, incarcare date, corectie date, corelare date, aprobare);
- Definire formulare electronice (aproximativ 30 de formulare cu o medie de 16-20 de campuri asociate);
- Definire rapoarte (rapoarte utilizator – aproximativ 60, rapoarte cu date agregate pentru analiza – aproximativ 40, rapoarte cu suport harta – aproximativ 20);
- Definirea continutului electronic static si dinamic de publicat in cadrul portalului;
- Definirea schemelor de salvare regulata a datelor/informatiilor din punct de vedere business;
- Definirea modalitatilor de indeplinire/aplicare a diverselor taskuri administrative;
- Elaborare detaliata a specificatiilor de integrare ale sistemului (se va integra cu minim 20 de sisteme/aplicatii informatice);
- Definirea specificatiilor de interfatare (se va interfata cu minim 10 sisteme/aplicatii informatice);
- Elaborarea specificatiilor de integrare ale Portalului cu celelalte componente ale sistemului, atat cele de baza cat si cele de suport a sistemului;
- Definirea specificatiilor pentru modulul „ajutor”;

- Elaborarea specificatiilor privind extinderea anumitor functionalitati ale portalului, precum si elaborarea specificatiilor privind implementarea unor functionalitati noi ;
- Elaborarea detaliata a cerintelor de performanta ale sistemului;
- Elaborarea detaliata a cerintelor non-functionale ale sistemului;
- Definitivarea rapoartelor pentru evidentierea indicatorilor de performanta ai sistemului si a anumitor categorii de utilizatori ai acestuia;
- Elaborarea propunerilor de optimizare (tuning) a sistemului;
- Elaborarea specificatiilor de deployment;
- Elaborarea specificatiilor scenariilor in vederea testarii;
- Elaborarea specificatiilor privind documentatia aferenta sistemului, pentru toate categoriile de utilizatori ai acestuia.

3.4 Componente de baza ale Sistemului

3.4.1 Modul Portal

3.4.1.1 *Experienta utilizator*

Pentru ca utilizatorii să aibă un singur punct de acces la resursele ce pot fi accesate pe web, se cere o interfață tip Portal care să strângă (agreghe) aceste resurse într-un singur loc, autentificarea utilizatorilor realizându-se doar la nivelul portalului și nu la nivelul fiecărei aplicații accesate. Un scop major al portalului este acela de a permite utilizatorilor, atât cât este posibil, să își administreze singuri modul de navigare și aranjarea conținutului în pagini.

Principalul scop al unei soluții moderne de portal este de a consolida multiple interfețe de utilizator provenite de la diferite sisteme și aplicații, și de a le face disponibile printr-un punct unic de acces web, unde utilizatorii se pot autentifica, pentru a avea acces la toate produsele și serviciile disponibile, în conformitate cu drepturile și rolurile lor din sistem. Modulul de portal va servi ca un punct de pornire pentru utilizatorii ce doresc să acceseze soluția. Astfel, interfețele de lucru către toate componentele soluției pot fi prezentate ca părți ale aceleiași soluții web, folosind diferite criterii de personalizare. Portal este în general

un site World Wide Web care se dorește a fi un punct de plecare pentru utilizatorii care se conectează la Web sau pentru vizitatorii care intenționează să-l viziteze.

Serviciile tipice oferite de portaluri cuprind directoare de site-uri web, facilități de căutare a altor site-uri, știri, informații despre vreme, e-mail, informații despre numere de telefon și uneori, forum-uri de discuții.

Termenul „portal software” desemnează un instrument de dezvoltare a portalurilor pe intranet-ul companiilor, astfel încât cetățenii să acceseze diverse informații precum e-mail, informații despre comunitate și hotărâri ale administrației locale și alte sisteme dintr-un punct central. Acest termen este similar și cu termenul „software pentru intranet”, dar diferă prin faptul că produsul final oferă o mai mare complexitate, automatizare, organizare și interactivitate.

Un Portal poate fi definit astfel: o interfață bazată pe Web, securizată, care oferă un punct unic de integrare pentru informație și accesul la ea, precum și pentru aplicațiile și serviciile utilizate de angajați, parteneri, cetățeni la nivel de organizație.

Principalul scop al unei soluții moderne de portal este de a consolida multiple interfețe de utilizator provenite de la diferite sisteme și aplicații, și de a le face disponibile printr-un punct unic de acces web, unde utilizatorii se pot autentifica, pentru a avea acces la toate produsele și serviciile disponibile, în conformitate cu drepturile și rolurile lor din sistem. Modulul de portal va servi ca un punct de pornire pentru utilizatorii ce doresc să acceseze soluția. Astfel, interfețele de lucru către toate componentele soluției pot fi prezentate ca părți ale aceleiași soluții web, folosind diferite criterii de personalizare.

În plus, o soluție de portal matura combina un mediu declarativ, bogat pentru crearea unei interfețe web, publicare și administrarea informației, accesarea datelor dinamice, și adaptarea experienței utilizatorilor folosind un framework pentru orice tehnologie web, cum ar fi accesul la aplicații bazat pe arhitectura J2EE și servicii web. Astfel soluția de portal are posibilitatea de a conecta angajații, partenerii și clienții cu informația de care au nevoie, și de a oferi vizualizări personalizate pentru fiecare comunitate de utilizatori.

Construcția paginilor și dezvoltările ce se realizează folosind modulul de portal, bazate pe instrumente ajutătoare, aduc administratorilor, dezvoltatorilor și utilizatorilor finali un mediu puternic în care pot crea pagini de portal complexe, cu un conținut variat și bogat, fără a fi necesară programare. Conținutul paginilor poate include atât portleti (componente reutilizabile ce expun informații provenite dintr-o sursă de date) cât și elemente de conținut (bucăți individuale de conținut: text, imagini, linkuri ce există pe o pagină de portal).

Organizarea și administrarea conținutului web este unul dintre beneficiile de baza în utilizarea unei soluții de portal. Funcționalități pentru gruparea paginilor în grupuri de pagini și pentru definirea șabloanelor de pagini dau administratorilor și dezvoltatorilor controlul necesar pentru a administra pagini și proprietățile paginilor. Setările de la nivel de grupuri de

pagini controlează șabloanele, paginile și tipurile de obiecte, proprietățile și clasificările elementelor de conținut, și traduceri lingvistice ce pot fi utilizate de paginile conținute în respectivul grup de pagini. Șabloanele de pagină oferă o modalitate puternică de a include conținutul standard al portalului (portletii și obiecte) și de a securiza stilurile predefinite, amplasarea în pagină și setările de securitate.

Portalurile moderne oferă funcționalități avansate de personalizare și customizare. Dezvoltatorii de pagini și administratorii pot controla nivelele de customizare al paginii și al portletilor, ce sunt disponibile pentru utilizatori: de la simple privilegii de ascundere, afișare și rearanjare până la privilegii ce permit construirea unei pagini. În plus, dezvoltatorii de portletii pot implementa o modalitate de customizare ce permite utilizatorilor să personalizeze conținutul și formatul portletilor, inclusiv abilitatea de a restrânge portletii ce sunt utilizați rar.

În plus față de securizarea accesului la orice tip de resursă web, modulul de portal oferă o interfață avansată pentru a administra utilizatorii din toate aplicațiile ce fac parte din portal, într-o manieră centralizată. Interfața web este construită peste un director LDAP ce aparține de componentă de securitate a soluției. Integrarea dintre aceste module asigură un grad ridicat de securitate pentru orice resursă găzduită sau accesată prin intermediul interfeței unice de utilizare.

Platforma Portal la nivel central trebuie să permită:

Accesibilitate:

- Accesul la pagina de Portal se va face printr-un navigator de Web de tip Internet Explorer, Mozilla Firefox sau Netscape;
- 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;
- Interfața web standardizată, simplă și intuitivă;
- Interfață cu utilizatorii bogată în funcționalități, care să ofere un nivel ridicat de accesibilitate, conform cu cerințele de accesibilitate WCAG versiunea 1.0;
- Interfață web cu template disponibile gratuit pentru look & feel comun organizației;
- Grad ridicat de securitate a sistemului, care să garanteze confidențialitatea și securitatea datelor utilizatorilor pentru accesul neautorizat atât din afară cât și din interiorul sistemului;

- Să ofere acces către toate resursele prezente în cadrul portalului printr-o singura autentificare, la deschiderea sesiunii;
- Sistemul de portal trebuie să ofere utilizatorilor versiuni diferite ale interfeței de portal, în funcție de tipul utilizatorului;
- Administrarea și dezvoltarea portalului se va putea realiza facil, utilizând doar un browser web;
- Platforma portal trebuie să furnizeze instrument dedicat de dezvoltare pentru aplicații web și portleți bazat pe platforma open source Eclipse.
- Instrumentul de dezvoltare trebuie să conțină componente software adaptate, ce generează cod (incluzând Java, JSP și XML) pentru o funcționalitate de aplicație specifică, astfel încât să se poată crea aplicații web sau portleți fără a fi nevoie de a se scrie cod.
- Soluția trebuie să ofere API-uri (Application Programming Interfaces) bine definite pentru integrarea cu aplicațiile existente.
- Dezvoltarea aplicațiilor trebuie realizată într-un mediu standardizat, ca de exemplu un mediu J2EE.
- Sistemul trebuie să conțină instrumente dedicate pentru construirea portleților
- Instrumentele de dezvoltare trebuie să ofere suport pentru următoarele standarde: XML, XSL, HTML, JSP, CSV.
- Soluția trebuie să ofere posibilitatea utilizării serviciilor web pentru a expune date și funcționalități către sistemele externe portalului.
- Soluția trebuie să permită comunicarea și notificarea evenimentelor între portleți.
- Trebuie oferită posibilitatea de a declanșa comunicarea între portleți la acțiunea utilizatorului sau automat în urma unui eveniment.
- Soluția trebuie să aibă o arhitectură deschisă.

- Sistemul trebuie să fie compatibil cu următoarele standarde în domeniu: WSRP, JSR-168, JSR-286
- Soluția trebuie să aibă la bază și alte standarde în domeniu, ca de exemplu: Java 2 Enterprise Edition (J2EE), XML, suport pentru servicii web.
- Sistemul să fie flexibil din punct de vedere al clienților de tip browser, al sistemelor de operare și al suportului pentru bazele de date.
- Administrare prin intermediu unui browser web.
- Sistemul trebuie să conțină mecanisme de tip asistent (wizard) pentru configurări avansate, cel puțin pentru configurarea cu sisteme de baze de date, mutarea bazelor de date, configurarea cu sisteme LDAP sau sistem de mesagerie instantanee.
- Suport pentru delegarea administrării pentru controlul accesului.
- Sistemul portal trebuie să permită folosirea de politici (colecții de setări) pentru administrarea următoarelor componente: utilizatori, grupuri, aplicații, web themes.
- Portalul trebuie sa contina propria componenta pentru managementul profilelor utilizatorilor.
- Portalul va permite utilizatorilor sa-si construiasca si sa actualizeze propriul profil, sa caute si sa gaseasca alti utilizatori pe baza unor criterii de cautare cum ar fi: nume persoana, departament, structura organizationala si de raportare, abilitati profesionale si domenii de interes.
- Portalul va permite utilizatorilor sa-si imbunatateasca vizibilitatea profilului in cadrul rețelei prin mecanisme de actualizare de status si taguri.

Interfata:

- Este necesar ca interfața portalului să fie separată, din punct de vedere logic, de codul aplicațiilor integrate, așa încât în cazul actualizării unei aplicației, să se păstreze toate particularizările ce fuseseră efectuate asupra interfeței.

- Trebuie să existe servicii de prezentare care să permită particularizarea interfeței pentru fiecare șablon de lucru sau rol din echipă.
- Utilizatorii trebuie să poată vizualiza, crea, converti sau edita documente, tabele de calcul și fișiere tip prezentare, direct din mediul de lucru portal, fără a avea nevoie de instrumente adiționale.
- Sistemul trebuie să ofere suport pentru crearea de portaluri virtuale, așa încât să se implementeze rapid sisteme adiționale tip portal, peste infrastructura existentă. Astfel se va utiliza o singură instalare de portal, peste care vor rula mai multe sisteme de portal diferite, cu URL-uri de acces diferite, grupuri de utilizatori diferite, elemente grafice pentru interfețe diferite.
- Interfața web a portalului trebuie să ofere o experiență de lucru utilizatorilor de tip web 2.0 incluzând tehnologii în domeniu cum ar fi AJAX, RSS Feeds, servicii REST.
- Conținutul accesat prin portal trebuie să fie automat afișat sau ascuns, pe baza rolurilor utilizatorilor, roluri care sunt predefinite.
- Utilizatorii trebuie să aibă posibilitatea de a particulariza pagina de intrare în portal, funcție de preferințe.
- Soluția trebuie să permită administratorului să specifice aplicațiile (portletii) obligatorii pentru paginile ce pot fi personalizate.
- Administratorii trebuie să poată controla drepturile utilizatorilor de a particulariza propriile pagini, funcție de rolul acestora, sau funcție de regulile definite.
- Utilizatorii trebuie să aibă posibilitatea de a adăuga portletii pe pagina prin funcționalitate drag-and-drop din paleta de portletii disponibilă.

3.4.1.2 *Continut electronic*

- Sistemul trebuie să permită crearea de șabloane de aplicații cu portleți direct din interfața web.
- Facilități de tip asistent creare site (wizard) pentru a crea rapid, din interfața web, site-uri web pe baza unor șabloane existente.

- Trebuie sa ofere posibilitatea de a crea, rula si administra facil diferite proprietati web, in acelasi timp permitand utilizatorilor de business, fara cunostinte tehnice avansate, sa poata administra siteurile web.
- Soluția trebuie să includă un instrument pentru publicarea de conținut, pentru a permite utilizatorilor privilegiați să publice, să actualizeze sau să șteargă propriile pagini, într-un mod simplu și facil.
- Soluția trebuie sa permită editarea conținutului direct in pagina in care este publicat.
- Pentru conținutului publicat trebuie să se stocheze data publicării, data la care trebuie arhivat și data la care documentul respectiv nu mai este valabil, cu scopul de a permite adăugări sau ștergeri automate.
- Trebuie sa ofere capabilitati de administrare centralizata pentru multisite-uri web, multi-lingvistice.
- Accesul la conținutul se va face funcție de utilizatorul care vizualizează datele – de exemplu, companiile externe organizației vor avea drepturi de acces la un conținut mai restrâns.
- Sa ofere suport pentru site-uri in mai multe limbi printr-o interfata simpla, usor de folosit pentru vizualizare „side-by-side” a paginilor in diferite limbi;
- Sa includa module si unelte usor de folosit care sa permita administrarea facila a continutului web, creerea de campanii de marketing online, sa permita optimizarea experientei web a utilizatorilor prin optimizari si prin optiuni de interactivitate;
- Formatarea conținutului trebuie realizată pe bază de șabloane (template-uri).
- Soluția trebuie să ofere capabilități de control al versiunilor și arhivare.
- Soluția trebuie să ofere posibilitatea de a extrage conținut direct din baza de date.
- Conținutul documentelor tip Word sau Excel sau a prezentărilor PowerPoint trebuie să poată fi integrat în mod simplu în sistemul de portal, prin portleți, fără ca

utilizatorii care vizualizează conținutul acestor documente să fie nevoiți să aibă instalate produsele Microsoft Office pe stațiile de lucru.

- Sa se integreze nativ cu aplicatii usuale din organizatii, cum ar fi aplicatii de tip CRM (customer relationship management), ECM (enterprise content management), e-commerce si altele, pentru a oferi o experienta online completa utilizatorilor.
- Sa permita utilizatorilor de business sa foloseasca actiuni de tip drag-and-drop pentru a include continut in contextul paginilor web, prin folosirea unei interfete de tip WYSIWYG.
- Sa includa capabilitati de autocorectie a textului introdus - spell checking.
- Trebuie sa includa un motor de reguli performant care sa permita utilizatorilor de marketing sa defineasca segmente de utilizatori si sa creeze reguli pentru ce tip de continut va fi livrat fiecarui segment de utilizatori online.
- Sa includa capabilitati analitice, care sa ofere date granulare pentru a putea identifica ce continut web si ce recomandari online sunt apreciate si folosite de segmentele de utilizatori online.
- Sa ofere posibilitatea de a optimiza continuu campaniile de marketing pentru a imbunatati gradul de utilizare si accesare a site-urilor, rata de conversie si loialitatea utilizatorilor.
- Interfața cu utilizatorul trebuie să ofere asistență pentru formatarea documentelor, astfel încât utilizatorii fără cunoștințe de HTML să poată contribui la publicarea de informații.
- Sa includa capabilitati avansate cu ecrane de previzualizare a site-urilor web , astfel incat utilizatorii sa poata vedea cum site-urile create vor aparea pe diferite tipuri de dispozitive mobile, incluzand aici toate modelele de iPhone, iPad, BlackBerry si Android.
- Trebuie sa ofere posibilitatea de a folosi in site-urile web date GPS pentru a oferi continut si servicii bazate pe locatia GPS. Site-urile web vor putea oferi astfel rezultate

ale cautarilor bazate pe date specifice regiunii unde se afla, recomandari si oferte bazate pe locatia respectiva precum si integrari cu harti online.

- Sa ofere capabilitati de administrare facila de cataloage complexe de date si resurse web.
- Soluția trebuie să suporte structuri ierarhice de navigare arborescentă pentru documente.
- Documentele trebuie să fie securizate fără a exista posibilitatea a fi accesate în absența autentificării.
- Sistemul trebuie să permită planificarea publicării de conținut.
- Soluția trebuie să asigure că structura de stocare este separată de structura de navigare printre documente (navigarea în site nu trebuie să reflecte în mod necesar modul de clasificare și stocare al documentelor).
- Soluția trebuie să ofere capabilități de publicare și personalizare de conținut direct dintr-un browser web.
- Trebuie sa ofere capabilitati avansate de uzabilitate si modalitati de contributie in site-urile web prin module ce permit utilizatorilor sa genereze continut si sa il administreze in site-ul web
- Trebuie sa ofere capabilitati de socializare si colaborare in site-urile web, prin includerea de functionalitati precum : comentarii, rating-uri, review-uri, sondaje si blog-uri, toate acestea trebuie sa fie puse la dispozitia utilizatorilor si sa poata fi administrate de acestia.
- Utilizatorii trebuie sa isi poata modifica/customiza experienta lor web in cadrul site-ului.
- Trebuie sa poata permite administrarea si managementul site-urilor web atat cele traditionale cat si cele pregatite pentru livrare pe mobil dintr-o singura interfata centralizata.

- Sa ofere suport pentru standardele SOAP, WSDL si UDDI.
- Sa ofere suport pentru standardele XHTML si HTML5.
- Trebuie sa fie compliant cu standardele W3C.
- Trebuie sa constituie o platforma de management continut web scalabila si stabila pentru a putea oferi o prezenta web la nivel national cu volume mari de trafic si utilizare;
- Trebuie sa includa un validator de cod pentru captarea erorilor in fisierele HTML, XHTML, XML, etc.
- Trebuie sa poata verifica si administra in mod automat link-uri interne sau externe invalide.
- Trebuie sa includa functionalitati de tip „gaseste si inlocuieste” continut (find and replace).
- Trebuie sa fie capabil sa importe/exporte fisiere XML si XLIFF.
- Trebuie sa suporte urmatoarele mecanisme de securitate : SSL, TLS, PKI.

3.4.1.3 *Formulare electronice*

- Soluția de formulare electronice trebuie să fie componentă a platformei portal propuse.
- Soluția de formulare electronice trebuie să fie compatibilă cu standardul de formulare xForms și să permită salvarea in format XML si importul XSD.
- Soluția de formulare electronice trebuie să conțină un instrument grafic pentru crearea de formulare electronice.
- Formularele electronice trebuie să poată fi accesate via web, prin intermediul unui browser web .

- Pentru utilizatorii care crează formulare, trebuie să existe un mecanism de tip asistent (wizard) care să ajute la crearea și proiectarea formularelor electronice.
- Sistemul trebuie să permită crearea de formulare tipizate similare cu formularele existente pe hârtie.
- Sistemul trebuie să permită colectarea de date în formularele electronice.
- Sistemul trebuie să permită transferul datelor colectate în formularele electronice către alte module.
- Sistemul trebuie să permită prepopularea formularelor electronice cu informații existente în baze de date folosind servicii standard, cum ar fi web services.
- Sistemul trebuie să permită semnături digitale și semnarea digitală a unui formular completat.
- Pentru situațiile în care mai mulți utilizatori lucrează pe același formular electronic, sistemul trebuie să permită fiecărui utilizator semnarea digitală secțiunilor din cadrul formularului care îi sunt atribuite.
- Sistemul trebuie să permită atașarea în cadrul formularului a unor documente existente în sistemul de fișiere.
- Sistemul trebuie să permită rutarea formularelor pe circuite de aprobare și să se integreze cu alte sisteme de workflow.
- Sistemul trebuie să permită salvarea datelor și a documentelor în mod independent, într-una sau mai multe baze de date.
- Sistemul trebuie să permită arhivarea documentelor create pe baza formularelor electronice.
- Sistemul trebuie să permită crearea de formulare care ajută utilizatorul la completare prin folosirea unui asistent de completare (wizard de completare formular).
- Formularele electronice disponibile pentru utilizatori trebuie să aibă o interfață prietenoasă, bazată pe standarde web 2.0.

- Unui formular electronic trebuie să i se poată aplica un template pentru interfața utilizator.
- Crearea unui formular trebuie să se poată realiza folosind șabloane de formulare predefinite sau create.
- Soluția de formulare electronice trebuie să fie independentă de o platformă sistem de operare și să poată funcționa pe platforme server Unix, Linux și Windows.
- Soluția de formulare electronice trebuie să fie independentă de un anumit sistem de gestiune baze de date relaționale și să poată funcționa în conjuncție cu cel puțin Microsoft SQL Server, Oracle sau IBM DB2.
- Soluția de formulare electronice trebuie să permită accesul cu mai multe tipuri de navigatoare web cum ar fi: Microsoft Internet Explorer sau Mozilla Firefox.

3.4.1.4 Fluxuri de lucru

Sistemul trebuie să înglobeze un motor (engine) de flux pentru creșterea flexibilității proceselor funcționale, oferind capacități puternice de rulare de fluxuri cu activități umane (interacțiuni cu utilizatorii). Acesta trebuie să ofere suport nativ pentru standardul BPMN precum și posibilitatea includerii de cod Java in-line direct în fluxurile de procese.

Fluxuri:

- Trebuie să permită implementarea de fluxuri secvențiale și paralele.
- Motorul de fluxuri de lucru să fie configurabil, permitând astfel utilizatorilor să definească procese de lucru, de aprobare a conținutului web pe baza proceselor de business.
- În cadrul procesului decizional există necesitatea de a împărți firul de execuție al lui flux normal în două sau mai multe fire de execuție, care să se execute în paralel în cadrul aceluiași proces.
- Trebuie să existe un punct unde subprocesele paralele (activitățile) converg într-un singur fir de execuție, sincronizând astfel mai multe fire de execuție.
- Subprocesele paralele converg într-un singur fir de execuție după anumite politici stabilite de către designerul fluxului.

- Definirea condițiilor de execuție de tipul AND și OR la nivelul tranzacțiilor compuse. În funcție de aceste condiții, precum și de ceilalți parametri existenți la nivelul acestor tranziții, motorul care execută aceste fluxuri poate decide care documente vor avea prioritate și când se consideră încheiate cele două fluxuri paralele.
- Funcționalitatea în cazul fiecărei decizii poate fi:
 - AND – se așteaptă execuția tuturor fluxuri secundare pentru a se continua;
 - OR – pentru a continua, se așteaptă terminarea oricărui flux din cele doua (tranziția compusă se consideră încheiată la terminarea oricarui flux secundar).

Activitati:

Activitățile sunt de 2 tipuri:

- Activități automate – se așteaptă rulearea unui proces al sistemului. Scriptul ce va rula este dat ca parametru în designer-ul de fluxuri. 2 activități automate pot fi considerate:
 - Transformare în PDF – este particularizare a activității automate, va fi o stare definită în designer (avantajul este că dezvoltatorul nu trebuie să știe care este scriptul de transformare în PDF);
 - Arhivare – este o particularizare a activităților automate, va fi o stare definită în designer. Această activitate va ține cont de configurarea pentru arhivare.
- Activități manuale – utilizatorul ia o decizie în ceea ce privește următoarea tranziție.

Tranziție:

Fluxurile secvențiale au următoarele tipuri de tranziții :

- (Ne)Procesat de toți;
- Întârziere;
- Respingere automată;
- Adaugă parametrii pe instanță;
- Adaugă parametrii pe document;

- Așteaptă răspuns;
- Verifică ultimul posesor al documentului;
- Decizie “Dacă”;
- Rutare ierarhică;
- Rutare dacă nu se găsește ierarhia;
- Adaugă un anumit posesor;
- Rutare la inițiatorul documentului.

3.4.1.5 Mesagerie instantanee

- Soluția de portal trebuie să conțină propriul sistem de mesagerie instantanee fără a fi nevoie de licențe suplimentare.
- Sistemul de mesagerie instantanee trebuie să permită chat și „presence awareness” din interfața web a portalului.

3.4.1.6 Server de aplicații

- Server-ul de aplicație trebuie să fie o platformă robustă și agilă ce oferă suport pentru rularea de aplicații J2EE, simplificarea dezvoltării, performanță ridicată și administrare inteligentă.
- Server-ul de aplicație trebuie să ofere suport pentru tehnologiile standard recente și cadre de dezvoltare menite să simplifice modelul de programare.
- Server-ul de aplicație trebuie să respecte standardul Java EE 6, să ofere suport pentru EJB 3.0, JPA (Java Persistence API) și JDK 6.0.
- Server-ul de aplicație trebuie să permită simplificarea interoperabilității prin suport pentru servicii web incluzând JAX-WS, SOAP 1.2, MTOM, XOP, WS-Reliable Messaging, WS-Trust, WS-Secure Conversation, WS-Policy, și Kerberos Token Profile.
- Server-ul de aplicație trebuie să ofere suport WEB 2.0 .
- Server-ul de aplicație trebuie să ofere suport pentru Session Initiation Protocol (SIP).
- Server-ul de aplicație trebuie să permită comunicare prin mesaje asincrone utilizând un provider integrat de Java Message Service (JMS), care respectă standardul JMS 1.1.

- Server-ul de aplicație trebuie să ofere suport pentru Java EE Connector Architecture (JCA) 1.5 pentru conectivitatea între serverele de aplicații și diferite Enterprise Information Systems (EIS).
- Server-ul de aplicație trebuie să ofere suport pentru Java Transaction API (JTA) 1.1 pentru gestionarea tranzacțiilor.
- Server-ul de aplicație trebuie să ofere acces autentificat și autorizat pentru a securiza funcții administrative și aplicații.
- Server-ul de aplicație trebuie să ofere suport pentru Resource Acces Control Facility (RACF) on z/OS, LDAP registry, Custom registry, file-based registry, sau federate registry.
- Server-ul de aplicație trebuie să ofere suport pentru Java Authorization Contract for Containers (JACC) 1.1, care să ofere securizarea resurselor gestionate de către server-ul de aplicație.
- Server-ul de aplicație trebuie să ofere suport pentru dezvoltare bazată pe modele cum ar fi Spring.
- Server-ul de aplicație trebuie să permită instalarea într-un singur pas.
- Server-ul de aplicație trebuie să ofere integrare nativă cu o platforma de dezvoltare compatibilă.
- Server-ul de aplicație trebuie să permită expunerea securizată a serviciilor intranet către utilizatorii de internet.
- Server-ul de aplicație trebuie să permită utilizare securizată a serviciilor web externe de către sistemele localizate în intranet.
- Server-ul de aplicație trebuie să permită structuri de cluster.
- Server-ul de aplicație trebuie să poată funcționa ca un server web, care să direcționeze cereri din browser către aplicațiile ce rulează pe server-ul de aplicații.

- Server-ul de aplicație trebuie să permită distribuție inteligentă a sarcinii de lucru în cluster.
- Server-ul de aplicație trebuie să poată realiza balansarea traficului ce intră în sistem.
- Server-ul de aplicație trebuie să ofere disponibilitate ridicată (high availability) și rezervă (backup) în interiorul clusterului.
- Server-ul de aplicație trebuie să ofere disponibilitate ridicată a tranzacțiilor și backup pentru tranzacții prin replicarea informațiilor referitoare la tranzacțiile în lucru pe toate nodurile active.
- Server-ul de aplicație trebuie să ofere mecanisme de reglare a performanței de la nivelul serverelor până la nivelul cel mai detaliat al aplicațiilor și al componentelor utilizate de acestea.

Acces universal de date și persistență:

- Server-ul de aplicație trebuie să suporte standardul Java Data Base Connectivity (JDBC) API 4.0 pentru conectare la orice tip de bază de date.
- Server-ul de aplicație trebuie să suporte Java Persistence API (JPA) pentru a asigura persistența și reutilizarea obiectelor.
- Server-ul de aplicație trebuie să suporte standardul Service Data Objects (SDO), pentru a accesa și manipula în mod uniform date din sisteme heterogene, sub forma de obiecte de colecții de structuri de tip arbore sau graph-uri.
- Server-ul de aplicație trebuie să suporte Portlets conform standardului Java Specification Requests (JSR) 286 (Portlet 2.0) .
- Server-ul de aplicație trebuie să suporte aplicații Session Initiation Protocol (SIP) conform standardului JSR 116.
- Server-ul de aplicație trebuie să suporte standardele Java Servlet 2.5 (JSR 154) și JavaServer™ Pages (JSR 245) .

Securitatea aplicațiilor:

- Server-ul de aplicație trebuie să ofere o granularitate ridicată.
- Server-ul de aplicație trebuie să ofere flexibilitate de definire și control al utilizatorilor.
- Server-ul de aplicație trebuie să ofere capabilități de auditare pentru a asigura respectarea regulilor și standardele existente în anumite domenii de activități.
- Server-ul de aplicație trebuie să permită implementări de tip secure proxy pentru a putea configura mai ușor serverul de aplicații când acesta este utilizat în DMZ.
- Server-ul de aplicație trebuie să ofere funcționalități Single Sign-On pentru interoperabilitate îmbunătățită între diferite aplicații și medii.
- Server-ul de aplicație trebuie să permită auditarea informațiilor de securitate a acțiunilor administrative, cum ar fi modificări de configurări de securitate, gestionare de chei și certificate , modificări de politici de control al accesului, etc.
- Server-ul de aplicație trebuie să ofere administrare a securității îmbunătățită la nivelul consolei de administrare, cu acces pe bază de drepturile în funcție de roluri la nivelul cell, node, cluster sau aplicație.

Administrare inteligentă:

- Server-ul de aplicație trebuie să permită anticiparea și ajustarea parametrilor critici pentru platformă.
- Server-ul de aplicație trebuie să ofere infrastructură simplificată și flexibilă pentru controlul eficienței mediilor de rulare.
- Server-ul de aplicație trebuie să ofere administrarea de la distanță a mai multor servere de aplicații.
- Server-ul de aplicație trebuie să ofere controlul mediilor complexe cu topologii complexe.
- Server-ul de aplicație trebuie să ofere activități administrative simplificate pentru aplicațiile de tip “multi-component”.

- Server-ul de aplicație trebuie să ofere o consolă de administrare web-base pentru gestionarea centralizată a tuturor componentelor din topologii ce includ mai multe servere de aplicații și/sau web.
- Server-ul de aplicație trebuie să permită gestionare centralizată a transferului de informații între medii cum ar fi: deploy, start, stop aplicații și distribuirea fișierelor în topologii ce includ mai multe servere de aplicații și/sau web.
- Server-ul de aplicație trebuie să ofere capacitatea de a realiza instalări centralizate către diferite medii remote.
- Server-ul de aplicație trebuie să ofere posibilitatea de a grupa și gestiona mai multe artefacte Java EE sub o singură definiție de aplicație.
- Server-ul de aplicație trebuie să ofere capacități de a configura cu ușurință securitatea și conectivitatea la baza de date și un client stand-alone pentru administrarea eficientă a mediului de deployment.
- Server-ul de aplicație trebuie să ofere scripturi avansate de administrare, care accelerează automatizarea implementărilor.
- Server-ul de aplicație trebuie să ofere capacități consolidate de administrare pentru dispozitive externe care pot fi integrate și gestionate în mediul de servere de aplicații.
- Server-ul de aplicație trebuie să ofere suport avansat de gestionare a resurselor ce constă în a alege doar funcționalitățile necesare pentru memorie și spațiu, în mod dinamic, în funcție de necesitățile aplicațiilor care rulează, pornind doar componentele necesare aplicațiilor ce rulează la un moment dat pe server și astfel reducând timpul de pornire și spațiul alocat server-ului.
- Server-ul de aplicație trebuie să ofere suport pentru noile standarde de Servicii Web cum ar fi:
 - Web Services Interoperability Organization (WS-I) Basic Profile 1.2 și 2.0;
 - WS-I Reliable Secure Profile;

- Java API for XML Web Services (JAX-WS);
- SOAP 1.2;
- SOAP Message Transmission Optimization Mechanism (MTOM);
- XML-binary Optimized Packaging (XOP);
- WS-Reliable Messaging;
- WS-Trust;
- WS-Secure Conversation;
- WS-Policy.

3.4.1.7 Control acces

Sub-modulul de control acces si management al utilizatorilor va oferi funcționalități de gestiune centralizata și automata a identificatorilor de identitate și drepturilor de acces asociate utilizatorilor în cadrul sistemului integrat. Acesta trebuie sa indeplineasca urmatoarele cerinte minimele:

- Sistemul trebuie sa permită autentificare bazata pe nume utilizator și parola, autentificare pe baza de certificat client SSL și autentificare folosind un subsistem terț destinat autentificării.
- Sistemul trebuie sa conțină propriile mecanisme de autorizare dar sa poată fi integrat și cu subsisteme terțe destinate controlului accesului.
- Sistemul trebuie sa permită administratorului sa creeze resurse, roluri și drepturi de acces care sa controleze ce utilizatori acces la diverse resurse pe baza rolurilor.
- Sistemul trebuie sa permită definirea de politici de acces care sa poată fi ulterior asociate utilizatorilor.
- Sistemul trebuie sa permită delegarea accesului pentru operațiuni administrative.
- Sistemul va fi capabil sa susțină definirea de reguli de acces la date (citire, scriere, ștergere și creare) pentru diverse grupuri de utilizatori.

- Sistemul trebuie sa permită configurarea rolurilor utilizator și a grupurilor și stabilirea drepturilor de acces pentru un utilizator în funcție de rolul sau grupul din care face parte.
- Platforma trebuie sa ofere capabilități pentru configurare a funcționalității de autentificare unica (“Single Sign-On”).
- Sistemul trebuie sa permită integrarea cu multiple registre majore de tip LDAP, cel puțin: Oracle ID, MS Active Directory, Tivoli Directory Server, Novel eDirectory, Sun Java System Directory Server.

3.4.1.8 Performanta

Scalabilitate si inaltă disponibilitate:

- Soluția trebuie să ofere posibilitatea de a implementa portalul într-un mediu cluster, având posibilitatea de a realiza balansarea încărcării, fără componente software adiționale.
- Soluția pentru portal trebuie să ofere capabilități de preluare a utilizatorilor pe un alt nod, în cazul unei căderi hardware (fail over).
- Sistemul portal trebuie să ofere capabilități tip “caching” pentru performanțe ridicate.
- Sistemul portal trebuie să ofere capabilități de cascada (rularea portalurilor multiple într-o singură imagine).
- Sistemul portal trebuie să ofere capabilități de federalizare (rularea portalurilor multiple în imagini multiple).
- Să permită suport nativ pentru realizarea serviciilor de cache dinamic fără necesitatea achiziționării de componente software suplimentare.
- Să permită instalarea componentelor de tip load balancer și server http pe mașini diferite față de instalarea propriu-zisă a portalului, pentru a asigura securitate și disponibilitate ridicate.

- Componentele pentru balansarea încărcării și cea de server HTTP trebuie să fie module componente ale serverului de aplicație pe care este instalat portalul.

Se vor include licențele de folosire a Modulului Portal care să ofere suport pentru utilizatorii acestuia, corelate cu modul de licențiere al producătorului, însă nu mai puțin de 4 procesoare folosite în componentele de multi-procesare simetrică din infrastructura hardware a sistemului.

3.4.2 Modul de Management al Documentelor

Componentele modulului de Management al Documentelor sunt:

- DMS – Componenta de Sistem de management al documentelor;
- Archive – Arhiva (de documente).

3.4.2.1 Sistem de management al documentelor

Este utilizat pentru stocarea documentelor și organizarea acestora în funcție de anumite criterii. Această componentă trebuie să ofere minim următoarele:

3.4.2.1.1 Caracteristici generale

- Modulul de management de documente trebuie să poată fi implementat independent de infrastructura de portal, astfel încât să beneficieze de propria arhitectură pentru înaltă disponibilitate.
- Modulul de management de documente trebuie să suporte cel puțin, următoarele platforme sistem de operare: Windows, Linux, Unix.
- Modulul trebuie să permită biblioteci de documente organizate pe directoare similare cu structura de directoare a sistemelor de operare.
- Trebuie să permită setarea de permisiuni la nivel de director din bibliotecă și rafinarea acestora la nivel de document în interiorul bibliotecii.
- Modulul trebuie să permită blocarea unui document pentru a fi editat (funcționalitate check-in/check-out), posibilitatea salvării ca draft înainte de publicare, crearea de versiune automată a lui și posibilitatea de revenire la o versiune anterioară, trimiterea spre aprobare înainte de a fi disponibil în biblioteca de documente.

- Modulul de management de documente trebuie să permită crearea de tipuri de documente specifice pentru organizație.
- Modulul de management de documente trebuie să permită previzualizarea documentelor de tip MS Office și PDF, direct din interfața web fără a fi nevoie ca utilizatorul client să aibă instalat pe stația sa MS Office sau alt software de tip Office Viewers sau PDF viewer.
- Organizarea și partajarea documentelor între persoanele aparținând aceluiași spațiu de lucru în echipă.
- Posibilitatea creării de spații de lucru în echipă (team spaces).
- Posibilitatea utilizării de bloguri.
- Posibilitatea creării de forumuri de discuții.
- Posibilitatea de a crea comunități de utilizatori bazate pe diverse criterii configurabile de către creatorul comunității.
- Posibilitatea de a adăuga documente în bibliotecile de documente direct din aplicațiile Microsoft Office sau echivalent, fără a fi nevoie ca utilizatorul să schimbe aplicația sursă a documentului.
- Posibilitatea de a acorda acces la bibliotecile de documente unor anume utilizatori sau grupuri de utilizatori.
- Posibilitatea de a crea biblioteci personale (private) de documente online pentru organizarea documentelor, având posibilitatea de a acorda acces la documentele din cadrul acestora utilizatorilor din cadrul unui anume team space.

3.4.2.1.2 Căutare

- Sistemul trebuie să implementeze o căutare după metadate cât și după conținut. Căutarea după conținut se face folosind motorul de indexare a binarelor.

3.4.2.1.3 Raportare

- Folosind sistemul de logare, metadatele asociate cât și documentele DMS trebuie să permită crearea de rapoarte standard dar și configurabile de către client.

3.4.2.1.4 Integrarea cu portal

- Trebuie să permită integrarea cu modulul Portal.

3.4.2.1.5 Integrarea cu sisteme tip Records Management

- Se poate face o integrare cu sistem de tip record management, sau se poate dezvolta o componentă internă, de record management.
- Sistemul trebuie să permită adăugarea de metadate particularizate, în funcție de necesitățile fiecărui client. Tot la nivel de se vor asocia și metadatele valabile pentru documentele conținute. Asocierea de metadate este configurabilă.

3.4.2.1.6 Procese automate de prelucrare a documentelor

- La nivel de DL se pot defini si procese automate de prelucrare a documentelor conținute. Procesele pot fi predefinite sau definite de dezvoltator(administrator) în funcție de necesități.

3.4.2.1.7 Lucru colaborativ

Permite implementarea unor metode colaborative pentru documentele conținute, prin:

- discutii gen Forum/Wiki /Blog
- trimiterea de notificări prin intermediul. mesageriei electronice în diverse situații de procesare a documentelor conținute (postare, actualizare, versionare, crearea unui topic). Destinatarii se aleg din listă sau sunt predefiniți la nivel de team space. Aici se pot activa/dezactiva notificările pentru acțiunile pe documentele incluse Document.
- Definirea de calendare de grup in cadrul unui team space pentru gestionarea comuna a activitatilor si sarcinilor de lucru atribuite in cadrul grupului.

3.4.2.1.8 Stocarea metadatelor

- Metadatele se țin la nivelul unei baze de date.
- Se vor implementa mai multe plugin-uri pentru mai multe sisteme de baze de date.
- Alegerea sistemului de baze de date se face la configurare.

3.4.2.1.9 Stocarea documentelor

- Binarele se pot ține la nivelul sistemului de fișiere al sistemului de operare, sau într-o bază de date.

- Se vor implementa mai multe plugin-uri pentru mai multe sisteme de baze de date. Alegerea sistemului de baze de date se face la configurare.

3.4.2.1.10 Funcționalități documente

Asocierea unor metadata

- Metadatale predefinite sunt:
 - Denumire;
 - Descriere;
 - Creat la;
 - Creat de;
 - Tag (un document poate avea unul sau mai multe taguri. Aceasta metadată poate ajuta categorizarea documentelor).
- Sistemul trebuie să permită adăugarea de metadata particularizate, în funcție de necesitățile fiecărui client.
- Asocierea de metadata este configurabilă.

Check In/ Check Out

- Check In:
 - lock pe Document
 - se marchează utilizatorul ce a făcut lock
 - dreptul de unlock îl are numai utilizatorul ce a făcut lock dar și Administratorul.
- Check Out:
 - unlock pe Document
 - în urma acestei acțiuni utilizatorul poate selecta dacă este o nouă versiune a documentului sau nu.
 - se marchează data modificării și utilizatorul care a făcut modificarea.

Lucru colaborativ

- permite trimiterea de notificări prin intermediul mesageriei electronice în diverse situații de procesare a documentelor conținute (postare, actualizare, versionare, crearea unui topic).
- Destinatarii se aleg din listă sau sunt predefiniți la nivel de DL.
- Notificările pot fi activate sau dezactivate la nivel de Document.

Publicarea conținutului

- Fiecare document stocat trebuie să aibă posibilitatea de a fi publicat. Prin publicare înțelegem actualizarea automată pe un anumit portal a conținutului documentului.
- Pentru aceasta produsul trebuie să implementeze un motor de convertire a documentelor în format HTML.
- Acest proces poate a fi apelat fie prin buton, fie dintr-un proces de flux după o anumită stare.

Urmărirea modificărilor din interiorului unor documente, și posibilitatea de "merge"

- Trebuie implementat un motor de conversie a conținutului în xml. Acest tip de conversie va ajuta sistemul să determine modificările efectuate la nivelul de paragraf.
- Conținutul xml poate fi afișat în format HTML pentru publicare sau dacă se solicită comparația dintre versiuni.

3.4.2.1.11 Interfata

- panoul principal trebuie să fie împărțit în zone configurabile cu acces la toate funcționalitățile puse la dispoziție de DMS.

Zonă "Sarcinile mele"

- Sunt afișate toate sarcinile utilizatorului.

Zonă pentru accesarea documentelor

- Permite navigarea utilizatorului în cadrul team space-urilor la care are acces.

- Documentele pot avea aceeași valoare pentru metadata categorie. În acest caz documentele se regăsesc în aceeași structură de directoare.

Zonă Favorite

- Se regăsesc toate Team Space-urile/Documentele ce au fost definite de utilizator ca fiind favorite

Zonă Forum

- Se accesează toate topicurile deschise pentru documentele la care participă utilizatorul.

Zonă Wiki

- Se accesează toate articolele deschise pentru documentele la care participă utilizatorul.

Zonă configurare interfață

- Se pot activa zonele de acces și poziția zonelor pe ecran.

Zonă administrare

- Se accesează controalele specifice de administrare.
- Această zonă este accesată numai de utilizatori care au dreptul de administrare.

3.4.2.2 Arhiva de documente

3.4.2.2.1 Medii de stocare configurabile

- Să permită integrarea cu mai multe sisteme de Storage Management Software (SMS). Crearea de plugin-uri pentru fiecare SMS.

3.4.2.2.2 Arhiva online

- Documentele arhivate pot fi restaurate imediat. Sunt mutate în locații diferite accesate direct de către utilizator.
- Toate documentele arhivate prin intermediul procesului de flux definit mai sus, vor fi stocate în arhiva online.

3.4.2.2.3 Arhiva offline

- Documentele arhivate pe benzi magnetice, sau în locatii unde utilizatorul nu are acces direct, si necesita interventia administratorului.

Se vor include licentele de folosire a Modulului de Management al Documentelor care sa ofere suport pentru utilizatorii acestuia, corelate cu modul de licentiere al producatorului, inasa nu mai puțin de 2 procesoare folosite in componentele de multi-procesare simetrica din infrastructura hardware a sistemului.

3.4.3 Sistem de Baze de Date Relationale

Componenta de sistem de baze de date relationale trebuie sa indeplineasca urmatoarele cerinte:

3.4.3.1 Caracteristici generale

- Baza de date relațională trebuie să suporte comunicarea cu aplicațiile client folosind protocolul de transport pe rețea TCP/IP.
- Baza de date relațională trebuie să opereze pe sisteme incluzand cel puțin Windows, Unix sau Linux.
- Baza de date trebuie sa suporte aplicatii scrise in limbaje procedurale SQL caracteristice mai multor sisteme de gestiune a bazelor de date.
- Baza de date trebuie să permită execuția de instrucțiuni INSERT de tip multi-tabelă.
- Baza de date trebuie să suporte tranzactii autonome.
- Baza de date trebuie sa suporte nativ stocarea si gestiunea datelor de tip XML.
- Baza de date trebuie sa ofere un mecanism inclus care sa permita interogarea istoricului modificarilor unei tabele fara a necesita dezvoltarea de triggeri sau rutine definite de utilizator, salvare periodica sau utilizarea functiei de audit.

3.4.3.2 Securitate

- Baza de date relațională nu trebuie să permită executarea de operații asupra obiectelor bazei de date decât dacă utilizatorul este autorizat pentru operația în cauză.

- Baza de date relațională trebuie să ofere o listă cu operațiile pe care un grup sau o clasă de utilizatori le poate executa.
- Baza de date relațională trebuie să ofere o facilitate care înregistrează informații despre modificări, inserări, ștergeri și selectări ale obiectelor bazei de date de către utilizatori individuali,
- Baza de date relațională trebuie să ofere abilitatea de a se ajusta la gradul de detalii, capturate de către facilitatea de audit.
- Baza de date trebuie să ofere mecanisme incluse de restricționare a accesului la date pe baza de etichete și politici de securitate.
- Baza de date trebuie să ofere mecanisme incluse de control granular al accesului la datele din tabele, la nivel de coloană, rând și la ambele niveluri.

3.4.3.3 Salvare și recuperare date

- Baza de date relațională trebuie să ofere o facilitate pentru salvarea întregii baze de date.
- Baza de date relațională trebuie să ofere o facilitate pentru restaurarea întregii baze de date.
- Baza de date relațională trebuie să ofere o facilitate pentru înregistrarea tuturor modificărilor bazei de date, pentru a permite recuperarea bazei de date (înregistrarea tranzacțiilor).
- Baza de date relațională trebuie să ofere o facilitate pentru recuperarea întregii baze de date la un moment din timp specificat de utilizator.
- Baza de date relațională trebuie să ofere abilitatea de a face salvări pentru unul sau mai multe spații alocate tabelor așa cum este specificat de către administratorul bazei de date.
- Baza de date relațională trebuie să scrie în mai multe fișiere pe disc simultan în timpul unei operații de salvare.

- Baza de date relațională trebuie să citească din mai multe fișiere pe disc simultan în timpul unei operații de restaurare.
- Baza de date relațională trebuie să permită citirea și scrierea paralelă în timpul unei operații de salvare.
- Baza de date relațională trebuie să permită citirea și scrierea paralelă în timpul unei operații de restaurare.
- Baza de date relațională trebuie să permită o arhitectură de înaltă disponibilitate.
- Performanța și scalabilitatea bazei de date.
- Baza de date relațională trebuie să permită folosirea ei în sisteme cluster.
- Baza de date relațională trebuie să ofere abilitatea să partiționeze tabele și indecsi.
- Baza de date relațională trebuie să permită unui tabel să fie partiționat bazându-se pe una sau mai multe valori specifice de date, așa cum este hotărât de către administratorul bazei de date.
- Baza de date relațională trebuie să permită definirea cantității minime de date transferate între disc și memoria locală a bazei de date la o cerere.
- Baza de date relațională trebuie să ofere facilitatea să rețină date din tabele special indicate în memoria locală pentru o perioadă nedefinită de timp.
- Baza de date relațională trebuie să permită setarea mărimii unei zone din memoria locală, rezervată să rețină date din tabele special indicate, pentru o perioadă nedefinită de timp.
- Baza de date relațională trebuie să aibă un optimizator bazat pe cost pentru a optimiza interogările.
- • Instanțe multiple, izolate, și complet funcționale ale bazei de date trebuie să poată coexista pe un singur nod SMP.
- Baza de date relațională trebuie să suporte indecși.

- Baza de date trebuie sa permita reorganizarea, mutarea si redefinirea de tabele fara blocarea activitatii.
- Baza de date trebuie să permita ajustarea automata, atat in plus cat si in minus, a memoriei alocate, in functie de cerintele din baza de date si de memoria disponibila in sistem.
- Baza de date trebuie să se ajusteze automat in cazul suplimentarii spațiului de stocare.
- Baza de date trebuie sa permita gestionarea dinamica a stocarii datelor in functie de frecventa de acces la date, astfel incat datele frecvent accesate sa fie stocate pe discuri rapide, iar datele mai rar accesate pe discuri lente.
- Baza de date trebuie să permita organizarea fizică a inregistrarilor din tabele in ordinea data de o coloană, mai multe coloane, si mai multe grupuri de coloane.

3.4.3.4 Integritate date

- Baza de date relațională trebuie să identifice și să rezolve situațiile de blocaj (deadlock).
- Baza de date relațională trebuie să permită administratorului să impună constrângeri de tip cheie primara.
- Baza de date relațională trebuie să permită ca o coloană să nu accepte valori NULL.
- Baza de date relațională trebuie să ofere abilitatea de a impune constrângeri asupra valorilor datelor.

3.4.3.5 Dicționar de date

- Baza de date relațională trebuie să ofere o facilitate de catalog (sau dicționar de date) care este modificată automat de fiecare dată când instrucțiuni de tipul Data Definition Language (DDL – Limbajul de definire a datelor) se aplică pe aceea bază de date.
- Baza de date relațională trebuie să ofere o facilitate pe platforma instalată pentru a accesa catalogul și a obține informații legate de obiectele bazei de date.

3.4.3.6 Administrare

- Baza de date relațională trebuie să ofere o interfață de administrare și dezvoltare a bazei de date.
- Baza de date relațională trebuie să aibă implementată o soluție internă a bazei de date pentru comprimare în momentul execuției operației de backup.
- Baza de date relațională trebuie să includă facilități de replicare între două baze de date de același tip.

Se vor include licențele de folosire a Sistemului de Baze de Date Relationale care să ofere suport pentru utilizatorii acestuia, corelate cu modul de licențiere al producătorului, însă nu mai puțin de 2 procesoare folosite în componentele de multi-procesare simetrică din infrastructura hardware a sistemului.

3.4.4 Platforma de Integrare a Componentelor

3.4.4.1 Infrastructura de integrare

Soluția oferită trebuie să conțină o infrastructură de conectivitate care să suporte servicii web și mesagerie JMS, oferind o flexibilitate mare prin implementarea interfețelor orientate pe servicii.

Această infrastructură va reprezenta componenta de conectivitate dintr-o arhitectură orientată pe servicii, oferind soluții de integrare bazate pe standarde deschise care să permită implementarea de soluții într-un mod rapid, prin reducerea complexității și numărului de interfețe dezvoltate. Infrastructura software de conectivitate va respecta cerințele detaliate de mai jos.

Sistemul ce se va dezvolta în cadrul proiectului va trebui să se interconecteze cu Sistemul Electronic Național, prin integrarea cu Punctul Unic de Contact Electronic (parte integrantă a SEN) conform legii 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice în mediul de afaceri, prevenirea și sancționarea corupției. Condițiile tehnice și de interoperabilitate prin care se poate realiza interconectarea vor fi puse la dispoziție de către MCSI.

3.4.4.2 *Server de integrare*

- Server-ul de integrare trebuie să permită conectivitate bazată pe servicii web și mesagerie JMS, oferind o flexibilitate mare datorita interfețelor orientate pe servicii.
- Server-ul de integrare trebuie să reprezinte componenta de conectivitate dintr-o arhitectură orientată pe servicii, oferind soluții de integrare bazate pe standarde deschise.
- Server-ul de integrare trebuie să permită implementarea soluțiilor cu ajutorul unui instrument de dezvoltare compatibil, ușor de utilizat, care nu necesită cunoștințe avansate de programare, instalarea, configurarea, dezvoltarea interfețelor făcându-se prin instrumente vizuale.
- Server-ul de integrare trebuie să ofere suport pentru integrarea cu o gama largă de tehnologii și aplicații.
- Server-ul de integrare trebuie să ofere flexibilitate în administrarea și configurarea de servicii.
- Server-ul de integrare trebuie să ofere un set larg de medieri gestionate prin politici și reguli.
- Server-ul de integrare trebuie să permită integrare cu un catalog de servicii, pentru gestionare politici și guvernare.
- Server-ul de integrare trebuie să permită selectarea în mod dinamic a End Point Web Service dintr-un catalog de servicii.
- Server-ul de integrare trebuie să ofere un mediu integrat de test pentru integrarea cu un catalog de servicii.
- Server-ul de integrare trebuie să ofere noduri native de jurnalizare a mesajelor primite dintr-o bază de date, oferind o interfață de configurare grafică, nefiind nevoie de programare.

- Server-ul de integrare trebuie să ofere o interoperabilitate sporită, oferind suport pentru WS-I Reliable Secure Profile, SOAP 1.2, WS-Reliable Messaging și standarde deschise.
- Server-ul de integrare trebuie să ofere capabilități de administrare simplificată a Qualities of Service prin seturi de politici Web Services.
- Server-ul de integrare trebuie să ofere un model de dezvoltare simplificată prin furnizarea unui nou mecanism de binding pentru Web Services bazat pe JAX-WS 2.0, JAXB 2.0, SAAJ 1.3 și StAX 1.0.
- Server-ul de integrare trebuie să ofere un model de dezvoltare simplificată bazat pe standardele SCA și SDO.
- Serverul de integrare trebuie să permită patern-uri de mesaje și protocoale, cum ar fi publish/subscribe, synchronous/asynchronous și topics/queues.
- Serverul de integrare trebuie să ofere suport complet pentru persistența mesajelor.
- Serverul de integrare trebuie să permită integrare la nivel de FTP, fișier și bază de date, nativ sau cu adaptori.
- Server-ul de integrare trebuie să ofere o flexibilitate sporită în scenariile service gateway.
- Server-ul de integrare trebuie să ofere o performanță sporită cu procesare paralelă pentru patern-uri de separare și agregare.
- Server-ul de integrare trebuie să ofere o posibilitate rapidă și ușoară de upgrade la o platformă de Business Process Management.
- Server-ul de integrare trebuie să ofere integrare cu orice provider de JMS și o automatizare pentru resursele JMS care rulează pe server.
- Server-ul de integrare trebuie să ofere posibilitatea de comunicare cu alte sisteme utilizând atât modele de programare bazate pe JMS cât și MQI.

- Server-ul de integrare trebuie să ofere suport pentru captarea și tratarea evenimentelor.
- Server-ul de integrare trebuie să ofere interacțiuni HTTP cu clienți de servicii RESTful și Servicii Web legacy.
- Server-ul de integrare trebuie să suporte transformări universale pentru formate de date complexe și standarde de industrie prin integrarea cu un motor specializat de transformare.
- Server-ul de integrare trebuie să permită export-import de diferite formate de date.
- Server-ul de integrare trebuie să suporte Web Services Notification pentru Servicii Web de tipul publish-and-subscribe.
- Server-ul de integrare trebuie să ofere posibilități de scalare pentru a permite creșterea numărului de procese și a utilizatorilor sistemului.
- Server-ul de integrare trebuie să suporte o arhitectura de tip cluster.
- Server-ul de integrare trebuie să suporte failover automat.
- Server-ul de integrare trebuie să ofere o balansare a încărcării la nivel web și aplicație.

Se vor include licențele de folosire ai Platformei de Integrare a Componentelor, corelate cu modul de licențiere al producătorului, însă nu mai puțin de 2 procesoare folosite în componentele de multi-procesare simetrică din infrastructura hardware a sistemului.

3.4.5 Platforma de Analiza si Raportare cu Suport de Harta

Platforma de raportare cu suport de harta include următoarele componente specifice:

- Server GIS - necesar pentru oferirea de servicii standard WEB-GIS (hărți tematice corespunzătoare indicatorilor de raportare) utilizatorilor interni și externi.
- Aplicație DesktopGIS - necesară pentru managementul și analiza datelor spațiale necesare raportărilor

- Harta de baza - necesara pentru oferirea unui background de calitate al aplicatiei webGIS si cautari spatiale dupa anumite criterii (exemple: pozitia unei localitati, a unui rau, a unui teritoriu administrativ, etc.)
- Aplicatie Web Gis - aplicatia WebGIS va pune la dispozitia utilizatorilor, prin intermediul browserelor standard (exemple: Internet Explorer, Mozilla Firefox) harta de baza si hartile tematice solicitate.

In capitolele urmatoare sunt detaliate cerintele minimale pe care trebuie sa le indeplineasca fiecare componenta in parte:

3.4.5.1 Server GIS

Serverul GIS trebuie să îndeplinească următoarele specificații minime obligatorii în vederea posibilității administrării datelor spațiale centralizat și dezvoltării de aplicații web cu suport GIS:

- Serverul GIS trebuie fie o soluție GIS scalabila, bazata pe platforma server, ce poate fi instalata pe un singur server pentru a deservi un număr restrâns de utilizatori, sau poate fi instalata distribuit pe mai multe servere pentru a asigura suport aplicațiilor beneficiarului;
- Să permită crearea, administrarea, si distribuirea de servicii WebGIS pentru a putea fi utilizate ca suport cartografic in aplicațiile WEB, desktop cat si pentru aplicațiile mobile;
- Să permită controlul asupra conținutului geografic printr-o administrare centralizata a datelor spațiale, inclusiv a imaginilor raster;
- Să permită transcalculul de coordonate “on-the-fly” din sistemul în care sunt stocate datele în cel în care sunt afișate;
- Să asigure accesul simplificat la serviciile WebGIS pentru profesioniștii GIS precum si pentru utilizatorii fara experiența in domeniul GIS;

- Să permită utilizarea datelor vector și datelor raster cu diverse rezolutii. De asemenea, utilizarea simultană, în aplicațiile web, a celor două categorii de date;
- Să ofere posibilitatea de particularizare, integrare și comunicare ținând seama de standardele internaționale specifice informației geospațiale și asigurarea interoperabilității Web;
- Sa permită indexarea automata si publicarea de conținut GIS la nivelul intregii organizatii;
- Integrare cu aplicațiile software desktop GIS, fără a fi nevoie de conversia datelor GIS și publicarea oricărei hărți realizate cu aplicațiile software desktop GIS;
- Să ofere suport pentru diseminarea informațiilor geospațiale și distribuirea capabilităților de cartografiere diferitelor tipuri de aplicații client, aplicații web de tip lightweight, aplicații de tip browser și aplicații desktop GIS;
- Să ofere acces la funcționalitățile GIS folosind o aplicație tip browser și posibilitatea publicării de servicii Web;
- Să ofere următoarele capabilități (cheie) de publicare pe Internet, precum:
 - randare de imagini,
 - interogare date,
 - extragere și descărcare date,
 - servicii WebGIS.
- Sa ofere funcții de integrare a datelor provenite din diferite surse, de pe Internet sau surse locale;
- Să permită utilizarea mai multor formate de imagine în crearea de cache-uri pentru serviciile de hartă publicate;
- Să permită crearea de “cache”-uri pentru serviciile WebGIS;

- Să ofere suport pentru publicarea temelor geospațiale ce au asociate informații temporale;
- Să permita publicarea bazelor de date geospațiale sub forma de servicii geospațiale, oferind astfel și accesul direct la aceste baze de date distribuite. Aceste servicii trebuie să ofere posibilitatea agregării într-o hartă a datelor spațiale provenite din baze de date geospațiale existente în cadrul unei rețele LAN, WAN și Internet.
- Să ofere funcționalități dedicate și instrumente specifice gestionării securizării datelor și serviciilor WebGIS și să asigure definirea utilizatorilor, a rolurilor și drepturilor de utilizare a datelor și serviciilor WebGIS dezvoltate. Modelul de securitate trebuie să permită limitarea accesului utilizatorilor neautorizați la datele și serviciile WebGIS;
- Să dispună de un set de instrumente dedicate optimizării și validării publicării rapide datelor și serviciilor WebGIS cu evidențierea într-o listă a erorilor sau a posibilelor proprietăți neadecvate ale straturilor de hartă;
- Să permită combinarea de servicii web de hartă multiple într-o singură aplicație web dezvoltată proprie;
- Să ofere un cadru de lucru scalabil pentru publicarea pe Internet a hărților interactive, datelor geospațiale, serviciilor WebGIS și accesul utilizatorilor la toate acestea, atât din cadrul organizației, cât și la nivel global.

3.4.5.2 Aplicație Desktop GIS

Componenta Desktop GIS vor avea în vedere acoperirea următoarelor necesități:

- Posibilitatea de a vizualiza și suprapune vectori și informații raster în diferite formate și proiecții;
- Posibilitatea de creare de hărți și explorare interactivă a datelor spațiale într-o interfață grafică prietenoasă;
- Posibilitatea de creare, editare și export date spațiale în formate standard;

- Efectuarea de analize spațiale (exemplu: operații algebrice pe hărți, analiza terenului, analiza rețelelor).

Uneltele GIS de introducere, editare și analiză informații geo-referențiate, inclusiv extensii vor permite crearea, editarea și analizarea informațiilor geo-referențiate de către utilizatori.

Licența software GIS desktop trebuie să permită utilizarea în mod concurențial (utilizatori multipli la momente de timp diferite).

Aplicațiile software desktop GIS desktop vor îndeplini următoarele caracteristici (cheie) generale:

- Să fie extensibile – posibilitatea adăugării funcționalității geospațiale specifice serviciilor și proceselor de lucru;
- Să respecte standardele internaționale ale informației geospațiale și să asigure interoperabilitatea cu sistemul IT, cu diferite sisteme DBMS, diferite formate standard de date vector și raster;
- Să permită customizarea aplicațiilor desktop GIS prin intermediul unor limbaje de programare standard ;
- Să ofere suport pentru cel puțin următoarele sistemele de operare:
 - Windows XP,
 - Windows Vista,
 - Windows 7.

Licența software GIS desktop trebuie să permită editarea, crearea și analiza datelor geospațiale și trebuie să îndeplinească următoarele caracteristici:

- Realizarea de hărți tematice profesionale și posibilitatea de tipărire, export în formate GIS, CAD salvarea și încorporarea acestora în alte aplicații sau documente;
- Gestionarea, crearea, utilizarea și organizarea datelor spațiale, datelor tabelare și metadatelor în vederea vizualizării, cartografierii, interogării și analizei spațiale ale acestora;

- Să dispună de instrumente de editare, culegere, întreținere, integrare, analiză, cartografiere și vizualizare a datelor geospațiale în cat mai multe formate diferite;
- Să includă instrumente și proceduri de analiză și geoprocesare oferind astfel evaluarea, interpretarea, compararea și înțelegerea cât mai corectă a procesului decizional folosind hărțile și informația geospațială;
- Să permită automatizarea și modelarea proceselor prin diagrame de analiză a datelor geospațiale;
- Să permită personalizarea interfeței utilizator prin adăugarea sau eliminarea barelor de instrumente.
- Să permită editarea de precizie ridicată cu ajutorul mouse-ului asemănătoare celei oferite de programele CAD;
- Să asigure instrumente pentru încărcarea obiectelor spațiale din OGC-WFS din baza de date geospațială și includerea acestor procese de prelucrare în modele de geoprelucrare și script-uri.

3.4.5.3 Baza de date spațială

Baza de date (geo-)spațială este o componentă absolut necesară derulării tuturor activităților ce exploatează informații geo-referențiate în cadrul soluției propuse. Permite salvarea, regăsirea, vizualizarea tuturor înregistrărilor în format GIS. Totodată asigură suportul pentru înregistrarea și tranzacționarea straturilor informaționale și a datelor de interes operativ în sistem GIS.

Baza de date geo-spațială trebuie să ofere următoarele caracteristici minimale:

- Să permită lucrul cu sub-queries;
- Să permită lucrul cu chei primare și chei externe;
- Să permită mosteniri (derivari) ale tabelor;
- Să permită lucrul cu triggeri;
- Să permită lucrul cu proceduri stocate;

- Sa permita lucrul cu tipuri de date spațiale.

Pentru baza de date geo-spatiala e necesară o soluție robustă și scalabilă capabilă să asigure disponibilitatea sistemului. Baza de date relațională trebuie să suporte comunicarea cu aplicațiile client folosind protocolul de transport pe rețea TCP/IP și eventual alte protocoale necesare.

Baza de date spațială trebuie sa indeplineasca urmatoare cerinte:

- Să fie o baza de date relaționala;
- Să poată rula pe arhitecturi de procesoare pe 64 de biți;
- Să asigure compatibilitatea cu standardul ANSI SQL;
- Trebuie să permită executarea de operațiuni SELECT, INSERT, UPDATE, DELETE;
- Trebuie să permită aibă suport pentru proprietățile ACID;
- Sa ofere posibilitatea de backup și restaurare a datelor în mod automat;
- Suport pentru stocarea diverselor tipuri de date si structuri de date, inclusiv pe tipuri de date XML;
- Suport pentru Unicode UTF-8 sau echivalent;
- Suport pentru proceduri stocate și triggere;
- Suport pentru căutare în câmpuri de text folosind șabloane de căutare;
- Să permită restricționarea accesului la obiectele bazei de date (tabele, view-uri, etc);
- Să includă mecanisme pentru restricționarea accesului utilizatorilor la date și obiectele bazei de date;
- Suport pentru replicarea bazei de date;
- Gestionare facila a obiectelor bazelor de date;
- Posibilitatea nativa de modelare a structurilor de date de tip arbore: metode incorporate pentru crearea și operarea pe noduri ierarhice;

- Posibilitatea stocării datelor binare mari, precum documente și imagini, ca parte integrantă a bazei de date, păstrând în același timp consecvența tranzacțională;
- Căutare complexă la nivel de text, folosind indecși specializați; efectuarea rapidă a căutărilor în acest tip de date;
- Suport pentru definirea datelor de tip spațial pentru consumul, extinderea și utilizarea informațiilor în aplicații activate din punct de vedere spațial. Datele de tip spațial trebuie să corespundă standardelor din domeniu, precum Open Geospatial Consortium (OGC).

3.4.5.4 Harta de baza

Harta GIS de baza ale sistemului vor oferi suport de afișare și căutare și vor conține minimal următoarele straturi. Baza de date vectorială va trebui să conțină, următoarele straturi cu atribute necesare afișării fără ca să se limiteze neapărat la acestea:

- rețeaua de drumuri;
- rețeaua de cai ferate căi ferate ;
- limitele unităților administrativ teritoriale ;
- limitele intravilanului localităților;
- râuri și lacuri (elemente liniare sau poligonale după caz);
- elemente de relief (vârfuri);
- utilizarea terenurilor (clasa: agricol, pădure, construit, etc.);
- puncte de interes;
- rețeaua de străzi ;
- relief umbrit;
- mozaic imagine raster.

3.4.5.5 Aplicația WebGis

Aplicația WebGIS pentru afișarea rapoartelor asociate indicatorilor și datelor asociate trebuie să îndeplinească următoarele cerințe specifice:

- Sa permită afișarea oricăror indicatori peste harta de baza:
 - Fiecare harta tematica generata pe baza unui anumit indicator sau combinație a acestora va putea fi afișata peste harta de baza ;
 - Vor putea fi afișate mai multe hărți tematice simultan.
- Să permită vizualizarea geografică a indicatorilor:
 - Să ofere operații specifice de operare a hărților: zoom-in, zoom-out, pan, zoom to full extent, zoom anterior, zoom următor;
 - Măsurarea de arii pentru poligoane, măsurarea de lungimi pentru linii, afișarea de coordonate pentru puncte;
 - Printarea hărții direct din pagina web;
 - Să furnizeze un mecanism de activare/dezactivare a straturilor astfel încât să fie posibilă vizualizarea și interacțiunea cu un singur strat sau cu un subset de straturi;
 - Să permită setarea de grupări de straturi care se exclud reciproc, pentru a nu afișa aceleași entități pe hartă în același timp;
- Să permită vizualizarea detaliilor alfanumerice asociate indicatorilor:
 - Să permită afișarea simultană a detaliilor alfanumerice și a reprezentării geografice;
 - Să permită afișarea tabelară a informațiilor pentru maximizarea informației vizualizate la un moment dat;

- Să permită afișarea paginată pentru a permite o navigare facilă atunci când listele de entitati devin foarte lungi.
- Să furnizeze un mecanism de selectare flexibil;
- Să permită filtrare în mod alfanumeric în funcție de atributele asociate entitatilor;
- Sa pună la dispoziție mecanisme pentru actualizarea hărții de baza :
 - Adăugare, modificare, ștergere entitati geografice;
 - Reactualizare de atribute alfanumerice.

3.4.5.6 Agregare si raportare

Platforma de Analiza si Raportare cu Suport de Harta trebuie sa aiba urmatoarele caracteristici specifice minimale:

- Sa includa un designer de rapoarte wip « WYSIWYG » ;
- Sa permita crearea de rapoarte “web-based”;
- Sa aiba o interfata tip « drag-and-drop » ;
- Sa contina mecanisme tip :
 - Tables ;
 - Dashboards
 - Crosstabs ;
 - Charts.
- Sa permita exportul de rapoarte in urmatoarele formate :
 - CSV ;
 - TXT ;
 - RTF ;
 - XLS ;

- HTML ;
- XML ;
- PDF .
- Sa permita crearea de sub-rapoarte in cadrul rapoartelor ;
- Sa ofere posibilitatea de « preview » a rapoartelor ;
- Sa ofere suport pentru fucntionalitati tip « Cut/Copy/Paste » ;
- Sa ofere suport pentru functionalitea undo/redo permitandu-se revenirea inaintea oricarei modificari in cadrul raportului;
- Sa ofere facilitatea de meniu sensibil la context ;
- Sa includa un “tool” dedicat pentru editarea obiectelor tip text;
- Sa includa un editor de expresii intuitiv;
- Sa includa documentatia de utilizare ;
- Sa ofere suport de tip « grid » si « snap to grid » ;
- Sa ofere suport pentru « rulers », « guides » si « snap to guides » ;
- Sa ofere suport pentru urmatoarele tipuri de surse de date, cum ar fi :
 - JDBC ;
 - XML ;
 - CALS table models ;
 - Hibernate ;
 - JavaBeans ;
 - EJBQL.
- Sa permita alimentarea cu date a unui raport din mai multe tipuri de surse de date ;

- Sa includa un repository tip « styles library » ;
- Sa ofere suport pentru « scriptlets » in definirea rapoartelor ;
- Sa nu limiteze dimensiunea rapoartelor sub o anumita valoare ;
- Sa ofere facilitati tip « properties view », « outline view » si “tasks view”;
- Sa ofere facilitati tip “Drill-through”, “hypertext links” si suport pentru “PDF bookmarks”;
- Sa ofere suport pentru vizualizarea in harta a indicatorilor agregati / calculati dinamic prin intermediul rapoartelor;
- Sa ofere posibilitati de stilizare grafica, prin folosirea simbolurilor si culorilor pentru rapoartele cu suport de harta;
- Utilizatorii trebuie sa aiba oportunitatea de a salva diverse stiluri create pentru reutilizarea lor la nevoie;
- Rapoartele cu suport harta trebuie sa permita recrearea ad-hoc a hartilor prin reclasificarea reprezentarilor, schimbarea simbolurilor si a paletelor de culori, etc.;
- Rapoartele cu suport de harta trebuie sa ofere minime facilitati de navigare precum zoom, pan si re-center;
- Rapoartele cu suport de harta trebuie sa se ofere si posibilitatea de creare a legendei;
- Rapoartele cu suport de harta trebuie sa poate fi salvate in format JPG, GIF si PDF;
- Tipuri de rapoarte suportate: tabelare, grafice, clasamente.

Se vor include licentele de folosire ai Platformei de Integrare a Componentelor, corelate cu modul de licentiere al producatorului, inasa nu mai putin decat echivalentul a 2 procesoare (folosite in componentele de multi-procesare simetrica din infrastructura hardware a sistemului) pentru sub-componentele Server GIS si Baza de data spatiala, precum si cate 5 licente utilizator pentru sub-componentele aplicatie desktop GIS si aplicatia WebGis.

3.5 Componente de suport ale Sistemului

3.5.1 Virtualizarea resurselor de procesare

Solutia va include o platforma de virtualizare dedicata, bazata pe Hypervisor propriu, fara dependenta de un sistem de operare anume. Aceasta solutie va fi instalata direct in platforma de procesare si va beneficia de suportul acestei platforme atat la nivelul capacitatii de procesare cat si la nivelul optiunilor de conectica si integrare cu restul elementelor de infrastructura.

Platforma de virtualizare trebuie sa fie compatibila cu toti producatorii hardware recunoscuti: IBM, Dell, HP, Sun, Intel, iar hypervisorul pe care aceasta platforma se bazeaza trebuie sa fie independent de producatorul sau de metoda de stocare interna/externa disponibila in platforma de procesare si/sau stocare pe care ruleaza.

Platforma de virtualizare trebuie sa ofere suport pentru urmatoarele sisteme de operare instalabile in masina virtuala: Windows Xp/Vista/7/2003/2008/2008 R2, Linux Suse/Red Hat/CentOS, FreeBSD, Solaris, Netware si sa permita adaugarea de spatiu de stocare pentru masinile virtuale prin folosirea urmatoarelor protocoale : NAS – NFS/CIFS ; SAN – iSCSI/FCP si prin folosirea urmatoarelor sisteme de fisiere : FAT32, NTFS, EXT2, EXT3, asigurand astfel compatibilitate cu majoritatea tehnologiilor implementate in mod uzual atat in platformele de procesare cat si in platformele de stocare.

Componentele virtuale ale platformei sa poata fi modificate cu usurinta permitand astfel crearea de configuratii diferite pentru seturi comune de masini virtuale, precum si crearea de configuratii unitare la nivelul intregii infrastructuri virtuale, atat din prisma elementelor virtuale de procesare si stocare (integrate nativ in platforma sau prin integrarea nativa cu componente terte ale respectivelor platforme de procesare si stocare), cat si din prisma elementelor de comunicatie (posibilitatea integrarii directe cu platforma de retea aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de retea si asigurarea crearii unei retele virtuale unificate la nivelul intregii infrastructuri virtuale).

Platforma de virtualizare trebuie sa ofere mecanisme proprietare pentru adaugarea de resurse de procesare si memorie fara restartarea sistemului de operare din masina virtuala, (in masura in care sistemul de operare suporta aceste facilitati), mecanisme ce pot fi independente de platformele de procesare/stocare/comunicatie sau prin intermediul unor conectori/componente comune respectivelor platforme.

Resursele virtuale (resurse de procesare, stocare si comunicatie) disponibile la nivelul intregii platforme de virtualizare (prin integrarea nativa cu platformele fizice de procesare, stocare si comunicatie) trebuie sa fie adresabile si configurabile in totalitatea lor prin intermediul unei singure interfete de management si nu prin configurarea separata pentru fiecare echipament disponibil in respectivele platforme.

Platforma trebuie sa permita gruparea si organizarea logica a resurselor de procesare in functie de necesitati, precum si izolarea acestor grupari de resurse, respectiv sa asigure flexibilitatea necesara maririi cantitatii de resurse disponibile intr-o grupare prin extragerea de resurse din alte grupari. Accesul masinilor virtuale si apartenenta la aceste grupari de resurse trebuie sa se faca atat in mod manual prin interventia unui operator cat si pe baza unor politici dinamice de acces.

Prin integrarea nativa cu platformele de procesare, masinile virtuale definite in platforma de virtualizare trebuie sa beneficieze concomitent de suportul a minim 8 procesoare logice, minim 256GB de RAM si acces la totalitatea porturilor I/O, resurse adresabile virtual prin abstractizarea resurselor fizice disponibile in infrastructura.

Platforma trebuie sa ofere mecanisme integrate de balansare a incarcarii resurselor fizice si virtuale disponibile in infrastructura si redistribuire a sarcinilor generate de utilizatori, servicii si aplicatii, prin integrarea nativa cu platformele hardware, indiferent de producatorul respectivelor elemente de infrastructura. Aceste mecanisme trebuie sa fie disponibile atat la comanda prin interventia unui operator cat si prin operatiuni automate definite in functie de necesitati, gradul de ocupare al resurselor si/sau pe baza unor reguli/politici prestabilite

Platforma de virtualizare trebuie sa ofere redundanta completa a arhitecturii, atat la nivelul elementelor virtuale distincte (procesoare, memorie, elemente de comunicatie, masini virtuale, etc) cat si la nivelul unor seturi intregi de echipamente de infrastructura (platforma de procesare, platforma de stocare, platform de comunicatie, etc) prin integrarea nativa cu mecanismele redundante existente in aceste platforme si prin folosirea unor tehnologii proprietare de redundanta, balansare si fail-over aplicabile intregului spectru de functionalitate asigurata (masini virtuale, servicii, aplicatii, platforme de procesare, platforme de stocare, platforme de comunicatie).

Platforma de virtualizare trebuie sa permita configurarea spatiului de stocare virtual prin integrarea directa cu platforma de stocare aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de stocare, mecanism ce va permite extinderea discurilor virtuale fara a fi necesara oprirea masinilor virtuale ce au atasate aceste discuri.

Prin integrarea cu resursele de management, platforma de virtualizare trebuie sa permita mecanisme integrate de mutare a masinilor virtuale de pe un server pe altul sau dintr-un datacenter in altul fara oprirea sistemului de operare ce ruleaza in masina virtuala si fara intreruperea serviciului oferit de aplicatia/aplicatiile din masina virtuala. Aceleasi mecanisme trebuie sa permita atat mutarea intregului harddisk virtual concomitent pentru oricare masina virtuala in cadrul aceluiasi datacenter sau intre datacenter-e diferite, independent de platforma de stocare folosita si de mecanismele de replicare ale acesteia, precum si extinderea automata a harddisk-urilor virtuale pe masura ce sistemul de operare si aplicatiile

din masinile virtuale o cer. In acest fel vor deveni posibile scenariile automate, prin politici pre-definite/definibile, de consolidare a masinilor virtuale pe un numar prestabilit de servere oprirea automata a serverele fara activitate sau cu subutilizare a resurselor de procesare.

Platforma trebuie sa includa o componenta de administrare si monitorizare dedicata, disponibila atat la nivelul echipamentelor fizice ce alcatuiesc platformele de procesare, stocare si comunicatie cat si la nivelul masinilor virtuale, ale resurselor virtualizate, aplicatiilor, serviciilor si protocoalelor insumate in infrastructura. In vederea accesului facil la functiile de administrare si monitorizare oferite, platforma trebuie sa permita acces atat prin consola locala/la distanta cat si prin browser web si prin platforma de management dedicata.

Componenta de management si monitorizare a infrastructurii trebuie sa permita autentificarea utilizatorilor bazata pe roluri si privilegii distincte de utilizare, prin integrarea cu un serviciu de tip director. Deasemenea trebuie sa permita crearea facila de politici dinamice de acces la resursele de procesare, precum si de disponibilitate ale acestora.

Separarea privilegiilor administrative trebuie sa se poata face pe orice element disponibil in interfata de administrare (server, utilizator, resursa de procesare, stocare, retea, etc), permitand astfel crearea de zone/domenii de securitate in functie de aplicatii si/sau roluri functionale, nu in functie de elementele disponibile in infrastructura de procesare, stocare si comunicatie.

Platforma de management trebuie sa asigure si mecanisme de definire si aplicare a profilelor standard de configuratie pentru serverele ce fac parte din infrastructura virtuala. Deasemenea sa permita configurarea de politici de aplicare a acestor profile in functie de necesitatile de moment sau in concordanta cu politica stabilita in prealabil.

Componenta de management trebuie sa se integreze nativ sau prin intermediul unor conectori/componente cu platforma de procesare si cu platforma de stocare in vederea realizarii operatiunilor de backup direct din aceste platforme, precum si pentru crearea rapida a unor zone izolate atat din punct de vedere al securitatii cat si al gruparilor de resurse de procesare, stocare si retea, in scopul testarii si dezvoltarii.

Se vor include licentele de folosire solutiei de virtualizare a resurselor de procesare, corelate cu modul de licentiere al producatorului, care sa ofere suport pentru toate procesoarele folosite in componentele de multi-procesare simetrica din infrastructura hardware a sistemului.

3.5.2 Confidențialitatea datelor

Una din soluțiile de securitate a Sistemului trebuie să asigure confidențialitatea informațiilor. Informația din acest sistem trebuie protejată împotriva amenințărilor în orice situație, fie când este stocată, fie când este transportată.

Principalele cerințe sunt:

- Sa fie independentă de platformă – să ofere suport pentru majoritatea sistemelor de baze de date relaționale.
- Sa fie independenta de producătorul bazei de date: nu se va baza pe logurile și nici pe auditul nativ al bazei de date.
- Sa fie accesibilă din locații multiple, în mod securizat, prin intermediul unei console web.
- Sa ofere scalabilitate ridicată, mergând de la protecția unei singure baze de date la protejarea a zeci de baze de date în centre distribuite.
- Sa permită accesul la modulele soluției și la date pe baza rolurilor.
- Sa includă un modul de management al rolurilor.
- Sa includă un singur repository centralizat la nivelul companiei pentru investigații.
- Sa centralizeze datele de audit în real-time, și nu la momentul creării de rapoarte, sau la un anumit interval de timp.
- Sa monitorizeze și sa aplice politici de acces privitoare la date sensibile, acțiuni privilegiate ale utilizator, controlul modificărilor, cererilor și activităților utilizatorilor precum și excepții de securitate, cum ar fi operațiuni eșuate.
- Sa permită crearea politicilor de acces la anumite tabele, pe baza userului cu care s-a autentificat utilizatorul la nivel de sistem de operare, pe baza adresei IP sau a adresei MAC, a protocolului de rețea, a momentului de timp în care a fost efectuată acțiunea, a aplicației sursă sau a tipului de comandă SQL.
- Sa trimită alerte în cazul violării politicilor de securitate.
- Să monitorizeze continuu toate operațiile asupra bazei de date, în timp real, detectând acțiunile neautorizate pe baza informației contextuale – “cine, ce, unde, când, cum” din fiecare tranzacție SQL.
- Politicile să poată fi adăugate facil prin intermediul unei interfețe intuitive.

- Soluția trebuie să ofere vizibilitate de 100% și granularitate a tranzacțiilor din bazele de date, prin monitorizarea următoarelor operații:
 - Excepțiile de securitate, cum ar fi erori SQL și autentificări eșuate;
 - Comenzi DDL gen Create/Drop/Alter Tables, care modifică structura bazelor de date;
 - Interogări SELECT ce pot avea impact asupra confidențialității datelor;
 - Comenzi DML (Insert, Update, Delete) care includ variabile;
 - Frazе XML executate de către baza de date.
- Să permită corelarea evenimentelor și actualizarea politicilor pe bază de comportament.
- Soluția trebuie să ofere totodată și:
 - Rapoarte predefinite.
 - Rapoarte care să ofere facilitatea de drill-down pentru identificarea problemelor.
 - O interfață grafică tip drag-and-drop cu ajutorul căreia să se construiască rapid rapoarte noi, sau să se modifice cele existente.
 - Facilități pentru transmiterea rapoartelor în mod automat, prin email sau sub formă de linkuri către pagini HTML. Aceleași rapoarte să poată fi vizualizate și online, prin consola web.
 - Posibilitatea ca logurile de audit trebuie să fie protejate față de acces implicit la nivel "root".
 - O funcționalitate de arhivare/restaurare a logurilor, cu criptarea arhivelor de loguri.
 - Integrare cu sisteme LDAP.
 - Suport pentru următoarele standarde: SNMP, SMTP, Syslog, CEF.

- Integrarea cu sisteme de tip Security Information and Event Management (SIEM).
- Configuratie de inalta disponibilitate pentru toate componentele solutiei.

Se vor include licentele de folosire a solutiei pentru asigurarea confidentialitatii datelor care sa ofere suport pentru necesitatile sistemului, corelate cu modul de licentiere al producatorului, incluzandu-se totodata, daca e cazul, echipamentele tip appliance dedicate.

3.5.3 Autentificare tip OTP

Suplimentar fata de autentificarea prin metoda « user name / password », sistemul informatic va trebui sa permita utilizatorilor-cheie (50 de persoane desemnate de catre Institutia Beneficiara), prin intermediul unui sistem specializat, autentificarea de tip « OTP – One-Time Password ». Aceasta metoda se bazeaza pe ideea ca parola folosita la autentificare este valabila pe perioada acelei sesiuni de lucru.

Sistemul de autentificare de tip OTP (« One-Time Password ») trebuie sa indeplineasca urmatoarele cerinte :

Generalitati :

Accesarea sistemului din locatia Beneficiarului se va realiza securizat prin intermediul Sistemului de autentificare tip OTP. Sistemul trebuie sa asigure autentificare de tip « two factor authentication », asigurand astfel protectie impotriva atacurilor de tip troieni, « man in the middle », « phishing », precum si pentru atacuri interne. Sistemul va prelua cererea de autentificare a utilizatorului, identitatea acestuia si parola dinamica, si o va trimite sistemului/serverului de autentificare OTP. Serverul de autentificare va verifica si va valida parola dinamica si va raspunde sistemului pentru continuarea interactiunii cu utilizatorul pe baza rezultatului procesului de autentificare. Validarea parolei dinamice de catre sistem asigura evidenta participarii utilizatorului respectiv, deoarece numai acesta cunoaste parola PIN precum si evidenta utilizarii echipamentului (token/card) asignat respectivului utilizator.

Avand in vedere numarul de utilizatori, cu niveluri de pregatire si profile eterogene, se va asigura o mare flexibilitate in configurarea solutiei, in conditii de performanta si costuri reduse. Pentru a asigura flexibilitatea solutiei, serverul de autentificare care valideaza parolele dinamice va trebui sa suporte echipamente si protocoale de autentificare multiple. Se solicita minim:

- Token hardware (minim 2 producatori diferiti cum ar fi Vasco, ActivIdentity sau echivalent);
- Carduri (ex. EMV CAP/DPA, Smartcard X.509 sau echivalent);

- Aplicatie de tip token pentru telefon mobil pentru utilizator (mobile token) in limba romana;
- SMS OTP;

Avand in vedere necesitatea de a proteja aplicatii cu caracter special, administratorii si utilizatorii care au acces la functionalitati de administrare si utilizare a Sistemului de autentificare tip OTP vor utiliza dispozitive de tip card, Sistemul de autentificare tip OTP asigurand totodata mecanismele tehnice necesare pentru a putea accepta mai multe tipuri de carduri.

Sistemul de autentificare tip OTP va asigura functionalitati/servicii de:

- Autentificare;
- Administrare.

Autentificare :

Avand in vedere drepturile de acces diferite la diverse resurse ale sistemului, solutia va asigura autentificarea diferentiata a administratorilor solutiei fata de autentificarea utilizatorilor.

- Autentificarea utilizatorilor in sistemul informatic se va realiza pe baza cererii primite si a validarii parolei dinamice introduse de catre utilizator;
- Fiecare tranzactie de autentificare (cerere si rezultat) va fi semnata digital si stocata in baza de date a serverului de autentificare;
- Solutia trebuie sa contina un mecanism implementat de prevenire a atacurilor de tip „brute force attack”
- Utilizatorilor li se permite accesul in sistem prin intermediul unui nume de utilizator si o parola dinamica OTP (One Time Password).
- Se va realiza restrictionarea accesului la informatie si la functionalitati in functie de drepturile de acces acordate fiecarui utilizator in parte.

Autentificarea administratorilor Sistemului de autentificare tip OTP si a utilizatorilor beneficiari :

- Autentificarea se va realiza prin utilizarea card-urilor de autentificare, in conformitate cu urmatorul flux de autentificare (dupa accesarea Sistemului de autentificare, utilizatorul va parcurge urmatoorii pasi):
 - Va apasa butonului de pe cardul personal de generare al parolelor OTP pentru generarea dinamica a „user name-ul” si ”OTP password” ;
 - Va introduce « user name-ul » si « OTP password » generate anterior ;
 - Serverul de autentificare va verifica cu ajutorul algoritmilor specifici daca parola este corecta;
 - Daca parola OTP introdusa de utilizator este validata si acceptata de catre componenta tip server de autentificare, se va permite accesul utilizatorului la portal;
 - In caz contrar, utilizatorul va trebui sa genereze o alta parola OTP si sa execute o noua incercare de autentificare.

Sistemul/serverul de autentificare va implementa metoda « Dynamic One-Time Password », metoda de generare a parolei OTP trebuie sa accepte atat versiunea « Event based » cat si versiunea « Time based » ;

Cardurile fizice utilizate pentru generarea parolelor OTP vor indeplini urmatoarele conditii :

- Respecta formatul “slim form factor” (pentru a fi usor transportat, sa incapa intr-un portofel obisnuit);
- Trebuie sa incorporeze un buton pentru comanda parolei OTP si un display luminos si cu contrast ridicat tip e-paper de 6-digit pentru afisarea acesteia (pentru utilizare facila in diverse locatii, in conditii de siguranta);
- Trebuie sa se ofere posibilitati de personalizare grafica a cardului pentru autentificarea OTP (astfel incat sa fie usor depistabila orice incercare de insusire, imprumut sau schimbare de carduri intre utilizatori de tip administrator si cursant, evitand astfel orice incercare de fraudă);

- Trebuie sa respecte standardele ISO 7810, ISO 14443, OATH, RoHS;
- Trebuie sa ofere o garantie de minim 3 ani sau 10.000 coduri generate.

Furnizorii vor asigura numarul necesar de carduri de autentificare pentru utilizatorii beneficiari de la MCSI, respectiv 50 de carduri de autentificare.

Sistemul de autentificare tip OTP trebuie sa includa un sub-modul de management al cardurilor pentru stocarea informatiile necesare referitoare la titularii cardurilor de autentificare, perioadele de valabilitate, statusuri, etc.

Administrarea sistemului/serverului de autentificare

Serviciile de administrare trebuie sa fie disponibile printr-o interfata Web si sa asigure minim:

Administrarea conturilor utilizatorilor si a proprietatilor de autentificare ale acestora :

- Configurarea proprietatilor de autentificare ca de ex :
 - Tipuri de autentificare;
 - Configurare hsm;
 - Managementul cheilor;
 - Parametrii de autentificare.
- Administrarea echipamentelor de autentificare:
 - Initializarea acestora;
 - Inrolare;
 - Monitorizarea starii / blocare;
 - Deblocare;
 - Sincronizare.
- Managementul conturilor utilizator:
 - Inrolare;

- Asignarea echipamentului de autentificare;
- Tiparirea parolei pin initiale;
- Monitorizarea starii / blocare.
- Managementul conturilor administrator:
 - Roluri;
 - Drepturi de acces.
- Statistici si rapoarte diverse:
 - Modul de audit .

Audit :

Se va asigura auditarea tuturor operatiilor efectuate in cadrul sistemului de autentificare OTP.

Facilitati de integrare, standardizare si interoperabilitate

Sistemul de autentificare tip OTP trebuie sa functioneze pe baza unei arhitecturi orientata pe servicii iar serviciile de autentificare sa fie furnizate ca servicii Web XML/SOAP, astfel incat sa se asigure mecanime standardizate de integrare cu infrastructura software, interoperabilitatea cu aplicatiile existente, contribuind astfel la asigurarea sustenabilitatii proiectului.

Pentru integrarea cu alte aplicatii/componente software se solicita disponibilitatea unui API standard care sa permita integrare peste canale SSL.

Sistemul de autentificare tip OTP trebuie sa asigure si acces prin protocol standard RADIUS.

Sisteme de operare si servere de baze de date suportate

Sistemul de autentificare tip OTP trebuie sa asigure disponibilitate pentru multiple sisteme de operare, precum :

- Microsoft Windows Server 2003/2008,
- distributii Linux.

Sistemul de autentificare tip OTP trebuie sa asigure disponibilitate pentru multiple sisteme de baze de date relationale, precum :

- Oracle Database,
- IBM DB2 ,
- Microsoft SQL Server 2005/2008.

Dispozitive hardware suportate

Pentru asigurarea flexibilitatii in implementare, compatibilitatea cu infrastructura hardware furnizata de beneficiar si minimizarea pe cat posibil a costurilor, solutia de autentificare va asigura disponibilitate pentru multiple echipamente HSM si telefoane mobile dupa cum urmeaza:

- Suport pentru echipamente HSM de la minim 2 producatori diferiti.

Sistemul propus pentru autentificare tip OTP trebuie sa fie o solutie consacrata pe piata. In acest sens, furnizorii vor prezenta in oferta tehnica minim trei exemple de implementari similare ale solutiei.

Furnizorii trebuie sa includa in oferta licentele de utilizare a Sistemului de autentificare OTP, corelate cu modul de licentiere al producatorului, si care sa asigure necesitatile de autentificare tip OTP pentru Sistemul Informatic.

3.5.4 Optimizare si control a accesului la servicii

Platforma va asigura un mecanism centralizat de control universal al accesului la serviciile de retea si de aplicatie, precum si la instantele sistem virtualizate. Controlul accesului la servicii se va exercita printr-un punct central de tip gateway, in configuratie redundanta de cluster formata din minim doua noduri hardware, si se va asigura pentru diverse scenarii de acces, inclusiv la nivel de segment de retea, prin tuneluri dedicate de acces limitativ la nivel de sistem sau de aplicatie individuala, precum si pentru accesul in mod portal la aplicatii interne.

Solutia va include suport pentru resurse complementare de autentificare, inclusiv de tip Single-Sign-On (SSO), si va permite integrare avansata cu alte servicii de tip server de autentificare, pentru extinderea unitara a politicilor de autentificare, autorizare si audit. Solutia va permite un nivel avansat de integrare cu componentele de management al identitatii si al accesului integrate in distributia de portal oferita.

Prin integrarea cu platforme standard, de tip directory sau platforme complexe dedicate (LDAP, RADIUS, Microsoft Active Directory, alte platforme de tip Kerberos), se va putea asigura gestiunea unitara a politicilor de autentificare si autorizare a accesului la resurse, inclusiv in medii de tip multi-domeniu si pe baza de cataloage structurate de tip directory multi-nivel.

Solutia va permite definirea flexibila si aplicarea stricta a politicilor de acces la resursele centrale protejate, si regruparea acestora la nivel de utilizator sau de grup de utilizatori, la nivel de terminal sau tip de terminal, si chiar la nivel de tip de conexiune sau de retea de acces si transport identificata, dar si pe baza de informatii de geolocalizare a terminalului fix, sau mobil.

Alaturi de mecanismele de tip interfata utilizator (grafica, web sau de consola interactiva), platforma ca include si un mediu de procesare complet instrumentat, pentru gestiunea avansata (programatic, scriptat, non-interactiv) a parametrilor relevanti ai platformei, dar si ai traficului obiect si ai politicilor de control respectiv aplicabile, la nivel de reguli de acces si in mod specific pentru fiecare protocol de aplicatie pentru care se asigura optimizare sau control al accesului. Platforma va dispune si de un set complet de tip SDK, pentru a permite integrarea in sisteme existente sau aflate in dezvoltare.

Mecanismele de autentificare suportate vor include in mod obligatoriu certificatele digitale pentru operator si, pentru toate cazurile in care tehnologia terminal utilizata o va permite, pentru terminalul utilizat.

Solutia va include sabloane de configurare (de tip wizard), dar si o interfata grafica de definire a fluxurilor si de editare a procedurilor asociate diverselor politici de autentificare si autorizare a accesului, inclusiv in ceea ce priveste tratarea exceptiilor si a erorilor, precum de definire a fluxurilor interne de audit la nivel de platforma.

Mecanismele de descriere completa, normalizata si parametrizata, utilizate vor face posibila configurarea si administrarea politicilor de autorizare dinamica a accesului la nivel de utilizator sau de grup, respectiv la nivel de tip de resursa protejata, in functie de contextul concret in care se solicita accesul.

Definirea mecanismelor dinamice de autorizare a accesului va utiliza structuri de tip ACL, cu variabile specifice pentru nivelul de transport si pentru cel de aplicatie al comunicatiei, si va putea fi facuta inclusiv la nivel de sesiune de acces.

Platforma de management a solutiei va putea corela datele agregate la nivelul componentelor hardware centrale, cu datele generate de componentele software client, pentru a permite alerte in timp real, dar si pentru a oferi rapoarte configurabile cu date de stare si cu statistici de utilizare. Rapoartele vor include date de utilizare normala, informatii de geolocalizare, dar si date despre anomalii si erorile de utilizare inregistrate.

Mecanismul de generare a rapoartelor va permite definirea cu usurinta a domeniului de interes specific, respectiv prin regruparea informatiei existente despre utilizarea sistemului de catre utilizatori si grupuri de utilizatori, precum si despre tipurile de resurse utilizate, la nivel de sistem si la nivel de terminal individual, pe tipuri de terminale.

Solutia va include componente de tip client software care vor putea fi instalate pe terminalul de lucru, fix sau mobil, si vor putea asigura detectarea tipurilor de retea disponibile, la care se terminalul se va putea conecta, in limitele politicilor de acces si de securitate configurate.

Politicile definite vor putea include atat utilizarea obligatorie de mecanisme specifice de autentificare, inclusiv multifactor, cat si aplicarea unui nivel specific de audit. Politicile vor putea include restrictii specifice de autorizare a accesului la resurse si in functie de postura de securitate a terminalului de pe care se solicita accesul, in cazul utilizarii de componentelor rezidente client.

Componentele client incluse vor permite memorarea zonelor de retea la care terminalul s-a conectat cu succes si vor putea asigura reconectarea automata, optimizarea transparenta si accelerarea comunicatiilor la nivel de client, fara a mai fi necesara interventia operatorului, exclusiv la retelele prin intermediul carora politica aplicabila va permite conectarea la resursele interne de retea, sau de tip portal, protejate.

Componenta client va oferi utilizatorului date despre nivelul curent de conectare, relativ la starea fiecărei conexiuni, precum si statistici despre tipul si volumul de trafic prelucrat, in date curente si referitor la istoricul utilizarii instantei client.

Componentele client incluse in solutie vor permite instalarea si utilizarea pe o varietate de platforme de tip terminale fix si mobil, cu suport specific la nivel de platforma de operare, cel putin pentru toate sistemele uzuale (Microsoft Windows, Linux si Mac OS, dar si pentru iOS si Android).

Solutia va permite, din punct de vedere tehnic, configurarea specifica a conectarii terminalelor si fara instalarea de componente client. In plus, ea va permite optimizarea si accelerarea comunicatiei atat intre site-uri, cat si intre concentratoare si clienti, si va asigura protectia criptografica a canalului de comunicatie in ambele scenarii.

Solutia oferita va permite conectarea de terminale din retele IPv4 la resurse aflate in retele IPv6, si invers, in mod transparent si fara a fi necesare componente sau licente suplimentare.

Solutia va permite asigurarea, direct de pe portalul inclus, a accesului la resurse de tip VDI in contextul aplicarii coerente a politicilor generale de autorizare aplicabile, si cu suport concurent pentru toate platformele majore relevante (cel putin pentru VMware View, Citrix XenApp / XenDesktop, Microsoft RDP).

Sistemul va permite afisarea dinamica, in mod portal, a legaturilor catre resursele de tip web la care utilizatorul autentificat are acces, in limita politicilor aplicabile, in mod specific pentru fiecare utilizator.

Mecanismele interne ale solutiei vor permite rescrierea dinamica transparenta a sesiunilor de tip Java applet, pentru a asigura controlul si protejarea oricarui flux de comunicatie asociat acestuia in interiorul canalelor protejate asigurate pentru aceasta, fara a fi necesara modificarea protocolului de aplicatie utilizat.

Solutia va permite definirea de zone protejate, in afara carora nici componentele sistem si nici utilizatorul nu vor putea crea fisiere, si in interiorul caruia sa vor regasi toate datele generate in contextul sesiunii de lucru. Toate datele din zona protejata vor putea fi criptate si decriptate transparent exclusiv pentru utilizatorul autorizat, iar datele temporare generate vor fi sterse la incheierea sesiunii.

Solutia va asigura optimizarea comunicatiilor la nivel de aplicatie web, prin resurse hardware si software la nivelul echipamentelor centrale si prin functii specifice ale componentelor client software.

Platforma oferita va include mecanisme de optimizare a comunicatiei WAN, inclusiv la nivel de protocol de aplicatie (CIFS, MAPI) si la incarcare / descarcare de fisiere, prin mecanisme de accelerare (deduplicare inteligenta, compresie adaptiva, caching dinamic) si management al alocarii specifice de resurse pentru fiecare tip de trafic de interes.

In mod specific, componentele client software vor asigura functii specifice de accelerare la nivel de client, inclusiv compresie dinamica locala si cache-client, dar si de definire de politici de tip QoS pentru prioritizarea traficului la nivel de aplicatie, inclusiv prin crearea de profile specifice pentru aplicatiile cheie.

Solutia va permite virtualizarea platformei de optimizare si de control al accesului prin partitionarea nativa a echipamentelor acestuia, ceea ce va permite configurarea de contexte administrative si de securitate distincte si functional independente, care vor putea deservi seturi de resurse diferite si care vor putea fi gestionate de echipe diferite, fiecare avand acces administrativ exclusiv la partitia alocata.

Solutia va putea fi extinsa ulterior, prin licentiere suplimentara si prin instante virtuale software functional identice, care vor putea fi instalate in medii virtualizate existente. Sistemul rezultat va putea fi administrat centralizat, in mod unitar si cu aceleasi resurse de management, atat pentru echipamentele hardware, cat si pentru instantele software virtualizate.

Solutia va fi dimensionata hardware si licentiata software pentru un catalog de 25000 de utilizatori unici si pentru a permite accesul concurent a cel putin 1000 din acestia la serviciile protejate.

Capacitatea de procesare a solutiei va putea fi extinsa cu usurinta, prin licentiere, pana la a asigura accesul concurent a cel putin 10000 de utilizatori, fara a fi necesare modificarea sau inlocuirea componentei sale hardware.

Pentru fiecare echipament hardware din componenta centrala a solutiei, se vor oferi configuratii care includ cel putin:

- Memorie interna: 8GB;
- Interfete de comunicatie:
 - 8 porturi 10/100/1000 Mbps, cu conectorizare RJ45;
 - 4 porturi 1Gbps, cu conectorizare pe fibra.
- Capacitate maxima de procesare specifica suportata:
 - La nivel de retea, 32 Gbps;
 - La nivel de transport, 4Gbps; 5000000 conexiuni concurente, in total, respectiv 175000 noi conexiuni pe secunda ;
 - La nivel de aplicatie, 4Gbps total, respectiv 50000 noi conexiuni pe secunda.
- Capacitate de procesare dedicata SSL (offloading) hardware: 15000 tranzactii pe secunda;
- Capacitate nominala de compresie: 3.2Gbps.

Se vor include licentele de folosire a solutiei care sa ofere suport nevoilor de optimizare si control a accesului la serviciile oferite de sistem, corelate cu modul de licentiere al producatorului, incluzandu-se totodata echipamentele de tip appliance ce vor fi dimensionate judicios, inclusiv in ceea ce priveste puterea de calcul de care dispun, si vor fi configurate pentru asigurarea functionalitatilor specifice in mod independent de alte module sau echipamente.

In configuratia oferita, modulele vor putea fi instalate in rack standard de 19inch, si vor dispune de surse de alimentare redundante.

3.5.5 Monitorizare acces la componentele sistemului

Se dorește o soluție care să asigure un nivel specializat din punct de vedere al monitorizării și al controlului accesului la componentele sistemului, care să se integreze cu acesta prin intermediul modului Portal.

Soluția se bazează pe un produs software care să combine controlul accesului la mașina a utilizatorilor, de la cei mai comuni, la cei privilegiați, respectiv a super-utilizatorilor. Astfel, Soluția permite importante reduceri de costuri de gestionare a utilizatorilor privilegiați, și de asemenea reducerea considerabilă a riscului de furt/sustragere a datelor din Sistem (organizație). Soluția trebuie să îndeplinească următoarele cerințe minime:

- Soluția trebuie să acorde accesul și controlul utilizatorilor privilegiați, oferind un control mai puternic al utilizatorilor privilegiați asupra modului în care pot accesa și utiliza datele instituției.
- Soluția trebuie să ajute la autentificarea utilizatorilor și să ducă la eficientizarea sistemului, reducând costurile de gestionare a utilizatorilor de sistem de operare, respectiv cont UNIX / Linux.
- Să genereze rapoarte privilegiate pentru fiecare utilizator, în deplină siguranță în câteva minute, ceea ce face mai ușor procesul de auditare.
- Să ofere facilitarea autentificării, accesul și controlul utilizatorilor de sisteme Linux/Unix la fel ca celor care fac parte dintr-un domeniu Windows.
- Să ofere acces securizat asupra întregii rețele hardware aferente proiectului.
- Sistemul trebuie să permită blocarea accesului pentru:
 - utilizatorii neautorizați;
 - utilizatorii autorizați care încearcă să acceseze elemente la care nu au acces.
- Să monitorizeze acțiunile și să identifice utilizatori care încearcă utilizarea greșită (în mod dăunător sau conștient greșit) a resurselor.
- Sistemul trebuie să abordeze deficiențele de securitate ale sistemului de operare prin oferirea de:

- segregare a sarcinilor pentru a se asigura accesul administrativ corespunzător;
 - date de audit detaliate ce urmăresc acțiunile până la aflarea identității reale a utilizatorului;
 - management centralizat al securității accesului pe tipuri diferite de platforme.
- Să permită definirea de entități operaționale (servicii TCP/IP sau terminale) și funcționale (realizarea unei anume tranzacții sau accesarea unei anume înregistrări într-o bază de date) pentru a fi monitorizate și securizate.
 - Sistemul trebuie să suporte sisteme de fișiere diferite printre care NTFS, FAT și CDFS.
 - Să aibă suport pentru IPv6, ce permite rularea în mediu hibrid IPv4-IPv6.
 - Să permită definirea accesului pentru utilizatori sau grup de utilizatori, în funcție de fișier, serviciu și funcții specifice la nivelul sistemului de operare (redenumire, copiere, pornire, oprire). Un utilizator autentificat al sistemului trebuie să vizualizeze doar acele facilități accesibile conform drepturilor sale.
 - Sistemul trebuie să poată adopta modelul de autentificare al privilegiului minim.
 - Să implementeze un model de control acces în funcție de roluri, de tip RBAC (role-based access control), un utilizator putând avea mai multe roluri concomitent.
 - Sistemul trebuie să furnizeze un set de politici predefinite care să adauge un nivel de securitate peste sistemul de operare.
 - Să permită propagarea în formă simplificată a politicilor la nivelul sistemului de operare.
 - Să permită crearea de politici prin moștenirea caracteristicilor altor politici, asigurând în același timp și propagarea schimbărilor.
 - Soluția trebuie să simplifice implementarea și gestionarea politicilor prin gruparea acestora logic pe seturi de politici aplicate în funcție de caracteristicile entităților asupra cărora sunt aplicate.

- Să gestioneze politicile de acces în cadrul unei ierarhii de servere și să aibă o interfață web de management a politicilor.
- Sistemul trebuie să permită carerea de politici pentru stabilirea parolelor pe baza unui șablon.
- Să fie capabil să descopere anomalii în stabilirea politicilor, permițând testarea politicilor definite înainte de a le implementa.
- Sistemul trebuie să permită controlul versiunilor politicilor.
- Siguranța sistemului trebuie să fie asigurată prin posibilitatea prevenirii autentificării multiple a unui utilizator.
- Sistemul trebuie să asigure posibilitatea prevenirii opririi neautorizate a rulării acestuia, de la distanță, modificarea sau ștergerea serviciilor și a datelor acestuia prin mecanisme proprii, asigurând astfel continuitatea protecției și controlului accesului.
- Să permită eliminarea necesității introducerii parolelor în codul aplicațiilor ODBC, JDBC și al fișierelor script, precum și controlul execuției programelor/aplicațiilor considerate a fi sensibile și monitorizarea tentativelor de acces.
- Sistemul trebuie să furnizeze mecanisme care să protejeze regiștrii sistemului de operare împotriva modificărilor, ștergerilor.
- Sistemul trebuie să permită prevenirea operațiilor de substituție/schimbare a unui utilizator sau grup (similar celor realizate în sistemele UNIX prin comenzile "setuid", "newgrp").
- Să realizeze criptarea comunicației între elementele sistemului utilizând SSL și AES (pe 256 biți), precum și a parolelor atât pentru utilizare cât și pentru stocarea acestora.
- Să furnizeze mecanisme de protecție împotriva "stack overflow", atacurilor tip "cal troian", atacurilor "worm" și mecanisme pentru prevenirea intruziunilor.
- Soluția să prevină operațiuni care pot fi dăunătoare sistemului ca: atacuri asupra parolelor (prin detectarea încercărilor de atac, prin prevenirea utilizării unor parole

slabe și prin prevenirea utilizării parolelor pentru un timp îndelungat), oprirea forțată a serviciilor/proceselor, implementarea parolelor și activarea securității în domenii NIS sau non-NIS.

- Să notifice în timp real asupra tuturor evenimentelor de securitate privind controlul și accesul în sistem.
- Soluția de control și acces să aibă o interfață cu utilizatorul care să permită accesul la unul sau mai multe stații protejate, de către administratorii de sistem, atât direct cât și prin rețea.
- Sistemul să aibă roluri predefinite, precum și roluri personalizate pentru toate tipurile de utilizatori.
- Soluția oferită să cuprindă agenți pentru fiecare stație, sistem protejat, de asemenea un modul de management al controlului și accesului, un modul de raportare, precum și modul de distribuție care să facă legătura între modulul de management și agenți.
- Soluția oferită să fie construită după o arhitectură de tip J2EE, care să permită integrarea cu module de tip UNAB (Unix Authentication Broker).
- Soluția să centralizeze într-o bază de date toate politicile de control și acces, toate rolurile, precum și toate conturile privilegiate, speciale.
- Managementul parolelor să fie făcut printr-un modul special inclus în soluția oferită.
- Soluția să conțină o componentă specializată pentru control și acces privind auditul și raportarea, atât în timp real cât și la cerere.
- Soluția integrată să suporte integrarea atât la nivel de PAM-Unix, precum și provizionarea cu alte containere de utilizatori, precum cele LDAP Active Directory.
- Soluția să suporte autentificare de tip AFS, respectiv să permită integrarea cu orice tip de mecanism de autentificare este furnizat soluției de control și acces.
- Soluția de control și acces să ofere autentificare de la terminal, respectiv stație precum și la nivel de aplicație.

- Solutia trebuie sa ofere utilizatorilor din domeniu facilitatea in care nu trebuie sa retina, respectiv sa foloseasca mai multe parole, singura utilizata sa fie cea de terminal, respectiv statie, indiferent de sistemul de operare rulat pe respectiva: UNIX, Linux, Windows.
- Solutia ofertat de control si acces sa centralizeze politicile de securitate astfel incat sa limiteze rolurile si drepturile administratorilor in sistem.
- Instalarea și mentenanța acestui software se va face de personal tehnic de specialitate al Prestatorului certificat de către producător - cel puțin 2 specialiști certificați de producator – (se vor prezenta diplome sau atestari) astfel încât să poata fi urmarite eventualele defectiuni și să fie remediate imediat ce au fost semnalate în sistem.

Se vor include licențe dimensionate pentru nevoile sistemului, corelate cu modul de utilizare al producatorului, incluzandu-se totodata si subscriptii pentru actualizări software din partea producătorului aplicației pentru minim 1 an fără costuri suplimentare din partea beneficiarului.

3.5.6 Autentificare pe baza recunoasterii semnaturii olografe

In vederea asigurarii unui grad ridicat de securitate al autentificarii administratorilor de sistem, se va implementa un sistem de autentificare si recunoastere a semnaturii olografe. Sistemul de recunoastere a semnaturii olografe trebuie sa indeplineasca urmatoarele cerinte :

- Inregistrarea utilizatorului in sistemul informatic prin stocarea in sistem de la acesta a unui numar de specimene de semnatura efectuate cu un device de tip « pix electronic » ;
- Recunoasterea semnaturii utilizatorului (semnatura originala) efectuata cu un echipament dedicat de tip pix electronic;
- Respingerea incercarilor de frauda prin imitarea semnaturii corecte a utilizatorului (adica respingerea accesului la semnalarea semnaturilor false).
- Nivelul de respingere a semnaturilor false sa fie de minimum 98 % ;

- Modulul trebuie sa tina cont in procesul de recunoastere a semnaturilor nu numai de aspectul grafic ci si de caracteristicile (acceleratiile) gestului utilizatorului reprezentat de semnatura.

Se vor oferi licentele de utilizare a sistemului de recunoastere a semnaturii olografe cu suport pentru 8 administratori ai sistemului, incluzandu-se totodata si echipamentele hardware tip pix electronic (dedicate). Pixul electronic trebuie sa indeplineasca urmatoarele cerinte tehnice :

Caracteristici fizice :

- Lungime pix: Minim 140 mm;
- Diametru pix: maxim 13 mm;
- Greutate: maxim 60 g;
- Formă ergonomică;
- Carcasă metalică;
- Tensiune de alimentare: 5V prin conexiune USB.

Componente incluse (minim) :

- Două microsisteme senzoriale de accelerație de tip MEMS (micro-electro-mecanical system) inerțiale, fiecare cu câte două axe ortogonale de sensibilitate;
- Microsistem senzorial autoreferențial de navigare optică pe suprafața de scriere;
- Microcontroler de tip AVR RISC pentru achiziția datelor captate de senzori.

Funcționalități :

- Captează semnale dinamice produse de mișcarea mâinii în timpul efectuării semnăturii olografe;
- Captează semnale dinamice produse de microvibrațiile de contact ale pixului cu suportul de hârtie pe care se semnează;
- Captează proiecția relativă a traiectoriei pixului, pe hârtia cu pattern de navigare imprimat;

- Comunicare cu sistemul de procesare și stocare a datelor prin conexiune USB 2.0;
- Odată cu achiziția datelor, se poate reține și semnătura în sens clasic, pe hârtie.

Funcționalități (oferite împreună cu componenta software de recunoaștere a semnăturii olografe) :

- Procesează semnalele dinamice produse de mișcarea mâinii în timpul semnăturii olografe
- Procesează microvibrațiile de contact ale pixului cu suportul pe care se semnează
- Oferă feed-back vizual, în timp real, către utilizator
- Stocază informațiile/semnalele asociate semnăturii într-o baza de date
- Procesează/compară semnalele asociate semnăturilor specimen inițial stocate în baza de date, cu semnalele asociate semnăturilor de intrare, stabilind în timp real, gradul de asemănare dintre acestea.

Uzabilitate :

- Semnătura se efectuează pe coli hârtie cu pattern pre-tipărit (se vor include minim 8000 de astfel de coli).

3.5.7 Salvare și restaurare date

Sistemul va include o componentă performantă pentru salvarea și datelor - produs software pentru protecția continuă a datelor cu posibilități de salvare în sistem de disaster recovery - care va îndeplini următoarele cerințe minime:

- Soluția trebuie să permită ca de pe aceeași consolă centrală să se poată administra mai multe locații.
- Soluția trebuie să fie modulară, cu posibilități de extindere.
- Soluția să fie certificată de producător.
- Soluția trebuie să dețină o consolă centralizată cu interfața grafică intuitivă.

- Accesul la consola trebuie să fie securizat cu autentificare bazate pe nume utilizator și parola.
- Sa se adreseze afacerilor desfasurate în medii eterogene.
- Consola centralizată trebuie să permita administrarea și monitorizarea mai multor servere de backup într-o rețea distribuită sau din locații aflate la distanță, precum și toate joburile și dispozitivele fizice de stocare existente pe aceste servere.
- Soluția trebuie să ofere suport pentru:
 - Sistemul de operare Microsoft Windows XP, Windows Server 2003 R2, Windows Server 2008 R2, 7 pe 32 de biți și 64 biți - inclusiv registrii și starea sistemului, precum și în configurații cluster,
 - Distribuții Linux,
 - UNIX.
- Soluția trebuie să permită instalarea remote a agenților și opțiunilor din consola de administrare.
- Soluția trebuie să permită administrarea dispozitivele de stocare din multiple locații fizice, inclusiv librăriile și mediile de stocare decuplate.
- Soluția să permită backup de tip mirror, backup care să poate fi realizat la locații diferite simultan, pentru a asigura un nivel ridicat de protecție a datelor.
- Soluția trebuie să permită administrarea extinsă a erorilor hardware, să corecteze erorile pentru a realiza completarea backup-ului, să permită detectarea și îndreptarea facilă a oricărui tip de eroare hardware.
- Soluția trebuie să permită utilizatorilor verificarea și corectarea problemelor legate de securitate, disponibilitatea mediilor de stocare sau a conexiunilor din rețea, înainte de a rula operațiunile de backup.

- Soluția trebuie să permita posibilitatea de a defini politici de filtrare și sabloane care să definească atributele job-urilor ce vor fi executate.
- Soluția trebuie să permita asistenți (wizard) pentru operațiile importante:
 - instalare,
 - creare joburi de backup/recovery,
 - formatare medii de stocare.
- Soluția trebuie să permita posibilitatea de a face backup pe o rețea secundară.
- Soluția trebuie să permita reîncercarea job-urilor esuate, cu rutarea lor către medii alternative.
- Soluția trebuie să permita notificarea automată folosind Microsoft Exchange, SMTP, SNMP și verificarea CRC (cyclic redundancy check) a datelor.
- Soluția trebuie să permită stergerea automată a log-urilor și cataloagelor vechi, cu posibilitatea de definire a perioadei de reținere pentru acestea.
- Soluția trebuie să permită posibilitatea de restaurare a sistemului de operare și a aplicațiilor deja instalate, inclusiv configurările existente, utilizând banda sau CD (tape/cd boot).
- Soluția trebuie să permită posibilitatea de a realiza backup de pe clienți (stațiile de lucru).
- Soluția trebuie să permită capacitatea de multiplexing ce permite până la 32 de servicii de scriere simultană pe același suport media.
- Soluția trebuie să permită utilizarea SAN-urilor Fibre Channel pentru backup și recuperare.
- *Opțiuni de Disaster Recovery* - Soluția trebuie să permită posibilitatea restaurării serverelor din rețea, fără a fi nevoie de reînștarea sistemului de operare sau softului de backup.

- *Opțiunea de Open Files* - Soluția trebuie să permită cu ajutorul acestui agent ca aplicațiile să poată rula fără întreruperi în timpul salvării datelor.
- Soluția trebuie să permită administratorilor să facă operații de backup și restore pentru device-urile de tip NAS. Soluția de backup să permită efectuarea backup-ului pe tape-uri sau librării atasate direct device-urilor NAS.
- Soluția trebuie să asigure protecția continuă a datelor și care să restaureze datele corupte de virusi, erori software sau erori umane prin capacitatea de a relua datele de la un moment imediat anterior înainte de coruperea acestora.
- Instalarea și mentenanța acestui software se va face de personal tehnic de specialitate al prestatorului certificat de către producător - cel puțin 2 specialiști certificați de producător – (se vor prezenta diplome, acorduri și/sau atestări) astfel încât să poată fi urmărite eventualele defectiuni și să fie remediate imediat ce au fost semnalate în sistem.
- Se va prezenta de către Prestator atestare pentru abilitatea de a susține traininguri cu personalul beneficiarului pentru produsele instalate în sistem.
- Se va prezenta de către Prestator o soluție demo care să prezinte modul în care cerințele enunțate au fost îndeplinite de soluția oferită.

Se vor include licențe dimensionate pentru nevoile sistemului, corelate cu modul de licențiere al producătorului, incluzându-se totodată și subscripții pentru actualizări software din partea producătorului aplicației pentru minim 1 an fără costuri suplimentare din partea beneficiarului.

3.6 Infrastructura hardware

În continuare, sunt prezentate specificațiile tehnice minimale ale platformelor și echipamentelor hardware de suport pentru Sistem:

3.6.1 Echipamente tip server

3.6.1.1 Platforma integrată de procesare

3.6.1.1.1 Suport fizic de tip rack pentru montarea și poziționarea echipamentelor (1 bucată)

Ansamblu modular standard de 19 inchi, cu 42U disponibili pentru poziționarea echipamentelor. Se vor include reperetele de montare necesare, inclusiv șine extensibile telescopic (sau soluții similare) cel puțin pentru echipamentele complexe de natura nodurilor de procesare, în scopul de a permite accesul fizic facil la componentele interne de tip hot-plug / hot-swap (surse, ventilatoare, plăci de extensie etc.) și deservirea acestora fără a fi necesară oprirea funcționării și/sau deconectarea echipamentului (ori de câte ori acest lucru este posibil din punct de vedere funcțional).

Structura internă a rack-ului va facilita poziționarea cablurilor, pentru distribuirea echilibrată a bugetului de conexiuni, respectiv pentru a implementa o schemă de asigurare a redundanței (la nivel de alimentare, interconectare SAN, LAN etc.) și evitarea condițiilor de tip single-point-of-failure.

3.6.1.1.2 Consolă de management general – (1 bucată)

Consolă locală KVM - unitate montată în rack, care va include:

- monitor TFT, de min. 17inch și suport pentru afișare de rezoluții native 1280x1024;
- tastatură USB cu dispozitive integrate de tip touch-pad și track-point;
- porturi de acces la consolele KVM și la porturile usb și video din nodurile de procesare astfel încât toate nodurile de procesare să fie deservite de monitorul și tastatura incluse în consolă (nu mai puțin de 6 porturi de acces KVM).

Pliată, consola va ocupa un spațiu optim de 1-2U în rack.

3.6.1.1.3 Surse neîntreruptibile (UPS) – (2 bucati)

Se va implementa o structură eficientă de alimentare de tip UPS compusă dintr-o unitate discreta independenta de tip on-line dublă conversie, monofazata (1/1) de 10KVA (8KW).

Aceasta structura trebuie sa ofere un timp de functionare in regim de avarie de minim 20 de minute la o incarcare preconizata de minim 50%.

Arhitectura preconizată este de natură sa aibă cost și complexitate minime, precum și un nivel optim de disponibilitate operațională; capacitatea preconizată și suportul de uptime vor permite acomodarea echipamentelor solicitate precum și rezerva necesară pentru extensiile ulterioare previzibile, fără a pune probleme de implementare.

Unitatea UPS trebuie sa permita extinderea timpului de functionare in regim de avarie prin cel puțin un modul discret de baterii, integrabil in structura fara necesitatea opririi alimentarii echipamentelor deservite.

Componentele interne ale unităților UPS, inclusiv bateriile, vor fi de tip hot-swap și vor permite deservirea (inclusiv înlocuirea acestora) fără oprirea sarcinii.

Unitatea UPS va include modul de management pentru monitorizare la distanță, inclusiv software de management si indicatori frontali pentru suprasarcina si nivel incarcare module de baterii.

3.6.1.1.4 Componente de distribuție (PDU) – (4 bucati)

Pentru alimentarea echipamentelor se vor folosi unități de tip PDU cu ieșiri tipice de 6A și conectorizare C13/C14.

Ansamblul va fi echipat cu numărul și structura de unități PDU, precum și cu cablurile aferente, necesare alimentării tuturor surselor echipamentelor instalate.

Interconectarea acestora se va realiza de așa manieră încât sursele care formează un set redundant, pentru același echipament, nu se vor alimenta în același PDU.

Această organizare are ca scop echilibrarea implicită a sarcinii precum și evitarea situației în care oprirea, accidentală sau planificată, a oricărei unități PDU să provoace oprirea alimentării oricărei surse în echipamentele critice echipate cu două sau mai multe surse și nici să nu necesite reorganizarea cablurilor pentru menținerea stării operaționale. Echipamentele critice echipate cu o singură sursă vor fi grupate în perechi redundante, oricare dintre ele capabil să preia sarcina sau să acopere funcționalitățile echipamentului pereche.

3.6.1.1.5 Șasiu modular pentru suportul procesării centralizate – (1 bucata)

Soluția/componentele oferite trebuie să îndeplinească următoarele cerințe generale:

- Sistemele și echipamentele livrate trebuie să fie noi, neutilizate și de ultimă generație. Ele trebuie să asigure gradul solicitat de performanță, fiabilitate și flexibilitate fiind proiectate și destinate pentru aplicații critice “enterprise level”.
- Dispozitivele hardware trebuie să fie astfel proiectate încât să poată asigura scalarea sistemului în cazul creșterii nevoii de putere de calcul.
- Dispozitivele hardware trebuie să fie compatibile cu caracteristicile rețelei electrice din România astfel încât să nu existe probleme la conectarea acestora la rețeaua electrică.

Arhitectura soluției propuse trebuie să includă următoarele caracteristici generale de fiabilitate, disponibilitate și ușurință în efectuarea service-ului (Reliability Availability Serviceability-RAS) la nivel de servere sau șasiu:

- componente redundante în interiorul sistemului (surse de alimentare electrică).
- capabilități de auto-testare și rezolvare a defectelor intermitente fără intervenție umană .
- dealocarea “online” și izolarea componentelor defecte ale sistemului (de exemplu discuri, ventilatoare, subsisteme de alimentare cu energie electrică, adaptoare PCI); în momentul reboot-ului componentele defecte vor fi deconfigurate
- diagnosticarea erorilor în timp real.
- capabilități arhitecturale de prevenire a erorilor .

Platforma de procesare reprezintă un ansamblu modular pentru suportul procesării, în arhitecturi mixte eterogene, format din șasiu modular și module de procesare:

- Componenta de tip șasiu modular pentru suportul procesării centralizate, cu suport pentru integrarea modulelor de procesare, a extensiilor de I/O ale acestora, precum și a modulelor de management.

- Șasiul trebuie configurat pentru instalarea de noduri de procesare de tip blade sau similare, optimizate pentru asigurarea densității și puterii de calcul necesare.
- Șasiul va fi echipat cu toate componentele redundante, hot-plug / hot-swap și utilizabile în mod concurent, pentru alimentare și ventilare, management (inclusiv procesoare de serviciu / management).
- Pentru asigurarea puterii de calcul necesare și adaptării la cerințele diverselor aplicații, fiecare șasiu va suporta configurarea și echiparea cu module (noduri) de procesare de tip blade pe 64 biți, în arhitectură CISC x 86 și/sau RISC, EPIC (sau derivate din EPIC).
- Șasiu montabil în cabinet sistem, cu suport pentru cel puțin 14 module blade, cu posibilitatea intermixării acestor module blade în șasiu în orice mod.
- Midplane de înaltă disponibilitate care suportă funcții de tip hot-swap la nivel de server blade individual, module de interconectare LAN, module de management, surse de alimentare.
- Suport pentru management de la distanță, redirectare interfața grafică, tastatura și mouse, posibilitate de pornire/oprire de la distanță pentru fiecare server blade, switch instalat, suport pentru remote media (virtual CD și floppy), suport pentru SSL (Secure Socket Layer).
- Unitate optică DVD-RW internă, pe panoul frontal, accesibilă de fiecare din serverele blade instalate în șasiu.
- Minim patru surse hot-swap, instalate intern în șasiu, redundante n+n, alimentare la 200-240 Vac. Sistemul va permite alimentarea concurentă a fiecărui modul sursă prin cel puțin 2 componente (căi de alimentare) intermediare PDU sau similare.
- Minim două porturi USB pe panoul frontal pentru unități media adiționale, accesibile de oricare dintre serverele blade instalate în șasiu.
- Sistem de ventilație de tip hot-swap, redundant, instalat intern în șasiu.

- Suport pentru minim opt module I/O interne pentru interconectare în tehnologie 1Gbps Gigabit Ethernet, 10 Gbps Ethernet, 8 Gbps Fibre Channel.
- Se vor oferi module de interconectare externa capabile sa maximizeze disponibilitatea ansamblului prin operare cat mai facila in caz de defectare minimizand necesitatea de reconfigurari LAN efectuate de administrator. Se solicita configuratii care sa asigure redundanta la defectare si No Single Point Of Failure.
- Minim 2 module ce vor asigura conectivitate externa prin minim 14 x 1 Gbps porturi Ethernet, cu capabilitati VLAN tagging, port mirroring, IGMP snooping si urmatoarele protocoale suportate: 802.1Q, IEEE 802.3ae, SNMP v2.
- Minim 2 module ce vor asigura conectivitate externa prin minim 14 x 10Gb porturi Ethernet fiecare, cu capabilitati VLAN tagging, port mirroring, IGMP snooping si urmatoarele protocoale suportate: 802.1Q, IEEE 802.3ae, SNMP v2, echipate cu minim 6 module de conectare SFP+ fiecare.

Componenta	Specificația tehnică minimală
Șasiu modular pentru suportul procesării centralizate - 1 buc.	
Tip, format	- Șasiu cu suport pentru integrarea modulelor de procesare, a extensiilor de I/O ale acestora precum și a modulelor de management. - Design modular, maxim 10U, montabil in cabinet de 19” cu toate accesoriile necesare montării incluse
Capacitate	Suport pentru minim 14 servere tip blade
Componente de acces la funcțiile de tip consola de management ale fiecărui modul de procesare	- Module de management centralizat pentru întregul șasiu, hot-swap, redundante 1+1, cu switch KVM încorporat pentru toate modulele de procesare de tip blade. - Suport pentru management de la distanță, redirectare interfața grafică, tastatură și mouse, posibilitate de pornire/oprire de la distanță pentru fiecare server blade, switch instalat, suport pentru remote media (virtual CD si floppy), suport pentru SSL (Secure Socket Layer), integrare LDAP (Lightweight Directory Access Protocol). - Modulul de management trebuie să dispună de porturi USB pentru tastatură și mouse, port VGA pentru conectare la monitor, port RJ-45 pentru management.
Consolă locală	Modul de tip KVM inclus, rack-mountable 1-2U, format din: - monitor TFT, de min. 17” și suport pentru afișare de rezoluții native 1280x1024

	<p>- tastatură USB cu dispozitive integrate de tip touch-pad și track-point.</p> <p>Consola va avea porturi de acces și interconectare cu consolele KVM din componentele platformei de stocare: min. 8 x porturi locale KVM/Cat5 pentru acces local.</p>
Subsistem de interconectare multi-path a componentelor de procesare și de stocare, în cabinetul sistem și în rețele locale LAN	<p>- Subsistemul va include componente discrete, implementate pentru configurare și operare independentă sau ca module în șasiul platformei de procesare</p> <p>- Atunci când acestea se vor implementa independent, porturile de comunicație individuale din fiecare modul de procesare de tip blade vor fi accesibile direct, din afara șasiului sub-sistemului de procesare, fără dispozitive intermediare de conectare, prin componenta neutră de tip pass-through.</p> <p>- Atunci când acestea se vor implementa ca module în șasiul sub-sistemului de procesare, vor dispune de cel puțin câte un port intern de conectare pentru fiecare modul de procesare blade pe care îl deservește.</p>
Surse de alimentare	2 module cu câte 2 surse de alimentare de minim 2200 W fiecare, hot-swap, instalate intern în șasiu, redundante n+n, alimentare la 200-240 Vac
Sistem de ventilație	Baterii de ventilatoare tip hot-swap, redundante, instalate intern în șasiu
Unitate optică	Internă, de tip DVD-RW, pe panoul frontal, accesibilă de fiecare din serverele blade instalate în șasiu
Porturi	Minim 2 porturi USB pe panoul frontal pentru unități media adiționale, accesibile de oricare dintre serverele blade instalate în șasiu
Module de interconectare LAN	<p>Minim 2 module ce vor asigura conectivitate externă prin minim 14 x 1 Gbps porturi Ethernet, cu capabilități VLAN tagging, port mirroring, IGMP snooping și următoarele protocoale suportate: 802.1Q, IEEE 802.3ae, SNMP v2.</p> <p>Minim 2 module ce vor asigura conectivitate externă prin minim 14 x 10Gb porturi Ethernet fiecare, cu capabilități VLAN tagging, port mirroring, IGMP snooping și următoarele protocoale suportate: 802.1Q, IEEE 802.3ae, SNMP v2, echipate cu minim 6 module de conectare SFP+ fiecare</p>
Standarde respectate	CE Mark (EN55022 Class A, EN60950, EN55024) CISPR 22, Class A, FCC Part 15 Class A

3.6.1.1.6 Componente de multi-procesare simetrică – (6 + 1 bucati)

Se solicită componente de multi-procesare simetrică, echipate cu procesoare CISC x86 multi-core cu următoarele cerințe:

- Modul de procesare de tip blade, compatibil cu șasiurile oferite;

- Minim 2x Intel Xeon Hex-Core, frecvența minim 2 GHz, 15 MB L3 cache sau echivalent;
- 128 GB PC3-10600 1333MHz ECC DDR3, suport pentru ChipKill sau echivalent, respectiv pentru configurare în mod hot-spare și pentru memory mirroring; fiecare modul va dispune de minim 16 sloturi de memorie în configurația oferită și va putea scala la minim 256 GB RAM prin extindere ulterioară;
- Controller video integrat;
- Interfețe de rețea dual 1 Gbps Gigabit Ethernet integrat, suport pentru failover și load balancing, suport TCP/IP Offload Engine (TOE);
- Interfețe de rețea dual 10 Gbps Ethernet integrat, suport pentru failover și load balancing, suport TCP/IP Offload Engine (TOE);
- Procesor de management integrat, capabilități de monitorizare a componentelor critice pe fiecare modul de procesare de tip blade, local și la distanță;
- Să includă funcții de diagnostic, reset, POST și auto-recuperare;
- Serverul va fi livrat împreună cu aplicația de management realizată de producătorul echipamentului, aplicație ce trebuie să asigure cel puțin: inventarierea componentelor, monitorizarea stării de funcționare, trimiterea de alerte prin e-mail;
- Modulul de procesare oferit trebuie să fie compatibil, certificat de producător și să dispună de suport pentru următoarele sisteme de operare: Microsoft Windows Server 2003 și 2008 Web/Standard/Enterprise, SUSE Linux Enterprise Server 11, Red Hat Enterprise 5 sau superior, VMware ESX 4.0 sau superior, Solaris 10.

Componenta	Specificația tehnică minimală
Componente de multi-procesare simetrică – 6 + 1 buc.	
Format	Modul de procesare de tip blade, compatibil cu șasiul oferit
Procesor	Echipat cu minim 2 x Intel Xeon Hex-core cu frecvența minim 2 GHz, 15 MB L3 cache, sau echivalent
Memorie internă	128 GB PC3-10600 1333MHz ECC DDR3, suport pentru ChipKill sau echivalent, respectiv pentru configurare în mod hot-spare și

	pentru memory mirroring; fiecare modul de procesare va putea scala la minim 256 GB RAM prin extindere ulterioară
Video	Controller video integrat
Interfețe de rețea	Echipat cu: - Interfețe de rețea Dual 1 Gbps Gigabit Ethernet, suport pentru failover și load balancing, suport TCP/IP Offload Engine (TOE) - Interfețe de rețea Dual 10 Gbps Ethernet integrate, suport pentru failover și load balancing, suport TCP/IP Offload Engine (TOE)
Management	- Procesor de management integrat, capabilități de monitorizare a componentelor critice pe fiecare modul de procesare de tip blade, local și la distanță - Suport pentru funcții de diagnostic, reset, POST și auto-recuperare - Serverul va fi livrat împreună cu aplicația de management realizată de producătorul echipamentului, aplicație ce trebuie să asigure cel puțin: inventarierea componentelor, monitorizarea stării de funcționare, trimiterea de alerte prin e-mail
Sisteme de operare compatibile, certificate de producător	Microsoft Windows Server 2003 și 2008 Web/Standard/Enterprise, SUSE Linux Enterprise Server 11, Red Hat Enterprise 5 sau superior, VMware ESX 4.0 sau superior, Solaris 10
Garanție și suport	Minim 3 ani
Unul dintre modulele blade va fi pentru management si trebuie sa fie echipat cu 2 HDD-uri SAS 600G	

3.6.1.2 Platforma de stocare consolidata multi-protocol - (1 bucata dual-node)

Solutia trebuie sa includa un sistem de stocare cu arhitectură internă flexibilă, în care nodurile active de control vor fi simultan conectate la toate structurile de tip bus sau loop (SAS loops și similare), pentru a face posibilă arondarea inițială și reconfigurarea ulterioară facilă a alocării discurilor între nodurile de control, între diferitele volume (sau structuri similare), precum și între servicii diferite (SAN/NAS).

Platforma de stocare va indeplini urmatoarele caracteristici :

- Echipamentul trebuie sa fie echipat cu doua controller-e in acelasi spatiu din rack pentru a putea dispune de o configuratie redundanta de tip cluster la nivelul echipamentului
- Echipamentul trebuie sa permita scalarea la minim 130 de discuri cu conectare de tip Serial SCSI (SAS) sau SATA.

- Echipamentul trebuie sa permita utilizarea in paralel a discurilor de tip SAS 3Gb/s si SATA II 3Gb/s.
- Capacitatile pentru un HDD minim disponibile trebuie sa fie de 1TB pentru discurile SATA si 600GB pentru cele SAS.
- Minim 6 GB memorie instalati si utilizabili pe sistemul de stocare. Memoria trebuie sa fie protejata cel putin cu acumulatori (baterie). In configuratie dual controller capacitatea maxima de memorie trebuie sa fie de minim 12GB.
- Minim 1 procesoare pe fiecare controller.
- Sistemul trebuie sa permita conectarea atat in standard File Access (NAS) cat si in standard Block Access (SAN).
- In configuratia livrata echipamentul trebuie sa fie echipat cu cel putin 8 porturi Ethernet cu o latime de banda de 1 Gb/s si minim 4 porturi Ethernet cu o latime de banda de 10 Gb/s.
- Echipamentul trebuie sa suporte utilizarea in paralel a urmatoarelor protocoale de acces si comunicatie: NFS, CIFS, iSCSI, FC.
- Sistemul trebuie sa suporte conectarea prin protocolul CIFS, NFS, iSCSI si FC la urmatoarele sisteme de operare: Microsoft Windows, Linux, SUN Solaris, in functie de suportul tehnologic oferit de fiecare sistem de operare in parte.
- Echipamentul trebuie sa suporte realizarea copiilor de tip Snapshot precum si replicarea datelor la distanta in mod sincron si asincron. Replicarea datelor la distanta trebuie sa fie suportata atata cu echipamentele din aceeasi clasa cat si cu cele din clasa diferite (inferioare sau superioare ca performanta) produse de acelasi producator.
- Unitatile de expansiune cu discuri trebuie sa fie compatibile cu sisteme de stocare din clasa superioara (scalabilitate si performanta) in asa fel incat in situatia unui upgrade/migrari inlocuirea acestora sa nu fie necesara.

In configuratia livrata echipamentul trebuie sa dispuna de urmatoarele functionalitati:

- Realizarea copiilor de tip instantanee - Snapshot, si posibilitatea de restaurare foarte rapida a acestora fara mutarea datelor salvate in copia de tip Snapshot ci prin remaparea blocurilor de date.
- Licenta inclusa pentru deduplicarea datelor.
- Configurarea si optimizarea matricilor RAID de tip RAID 0, 1, 5 6 si combinatii.
- Conectarea prin protocol iSCSI sa fie disponibila in configuratia initiala.
- Conectarea prin protocol NFS sa fie disponibila in configuratia initiala.
- Conectarea prin protocol CIFS sa fie disponibila in configuratia initiala.
- Sistemul trebuie sa fie echipat in configuratia livrata cu minim 24 de discuri SAS cu o capacitate de 600GB pentru fiecare disc. In aceste conditii spatiul ocupat in rack nu trebuie sa depaseasca 4U impreuna cu controller-ul sistemului de stocare.
- Licenta software care sa asigure monitorizarea performantei si capacitatii platformei de stocare atat la nivel fizic cat si la nivel virtual. Solutia software trebuie sa asigure functionalitatile respective atat pentru platforma existenta cat si pentru alte platforme de la acelasi producator sau de la producatori diferiti, platforme ce pot face obiectul unor achizitii ulterioare. Solutia trebuie sa indelineasca urmatoarele cerinte:
 - Sa monitorizeze performanta platformelor de stocare existente si sa identifice blocajele de performanta atat la nivelul serverelor fizice si virtuale conectate la volumele de date cat si la nivelul volumelor de date exportate catre platformele de procesare
 - Sa permita izolarea surselor de blocaj al performantei si oferirea de solutii alternative de acces la volumele de date si la capacitatea disponibila pe discuri, astfel incat aceste blocaje sa poata fi usor depasite
 - Sa permita automatizarea proceselor de planificare a capacitatii de stocare prin mecanisme de colectare datelor relevante privind numarul de discuri, lun-uri, volume de date, cai de acces, grad de ocupare al resurselor de

procesare si al capacitatii de stocare, respectiv predictie pentru gradul viitor de ocupare al acestor resurse, prin analiza predictiva a tuturor parametrilor enumerati

- Sa permita vizualizarea facila a tuturor parametrilor rezultati in urma proceselor de planificare si predictie
 - Sa permita procese automate de corelare a masinilor din platformele de virtualizare, a aplicatiilor si a conexiunilor logice cu spatiul fizic de stocare disponibil in platformele de stocare
 - Sa permita clasificarea datelor aflate in platforma de stocare, prin identificarea tipurilor de fisiere si a istoricului de acces catre aceste fisiere
 - Functionalitatile descrise trebuie sa fie disponibile atat pentru platforma existenta cat si pentru platforme SAN (incluzand echipamentele de comunicatie de tip fabric SAN si echipamente de conexiune de tip HBA) de la alti producatori majori de platforme de stocare, platforme ce pot face obiectul unor achizitii viitoare.
 - Sa permita agregarea datelor de la platforme eterogene (multi-vendor) de stocare intr-o singura interfata de administrare, vizualizare si raportare.
 - Sa permita vizualizarea si raportarea capacitatii de stocare, alocarii si utilizarii capacitatii de stocare la toate nivelele platformei de stocare (raw, RAID, LUN, volume de date si sisteme de fisiere).
- Grantie de minim 36 de luni inclusa in configuratia propusa. Suportul si garantia trebuie sa fie asigurate in Romania de producatorul echipamentului de stocare.

Componenta echipamentului	Specificatia tehnica minimala solicitata
Arhitectura	Cluster Activ-Activ de 2 noduri (controller-e)
Protocoale SAN	IP SAN (iSCSI)

Protocoale NAS	NFS V2/V3/V4 peste UDP sau TCP, PCNFSD V1/V2 pentru (PC) autentificarea clientilor NFS, Microsoft® CIFS, CIFS
Numar de LUN-uri	Minim 1000
Numar de volume	Minim 1000
Numar de servere host conectate direct	4 in conexiune directa, 256 in conexiuni prin mediu de comunicatie de tip fabric
Tip conectivitate pentru disk-uri	Minim Dual-Path/Multi-Path pentru asigurarea suportului de inalta disponibilitate
Interfata de management dedicata	Minim 1 port de consola integrat Full-duplex 10/100 Base-T Ethernet
Porturi Gigabit Ethernet	Minim 8 x Full-duplex 10/100/1000 Ethernet
Porturi 10 Gbps	Minim 4 x Full-duplex 10 Gbps Ethernet
Memorie totala	Minim 12 GB ECC
Disk-uri suportate	SAS : 300 GB, 600 GB SATA : 1 TB, 2 TB, 3 TB
Disk-uri echipate	24 x HDD SAS 600 GB la 10000 rpm
Capacitate utila de date	Minim 12 TB
Nivele RAID	RAID 0, 1, 5, 6 și combinații
Sistem de operare	Proprietar producatorului echipamentului de stocare
Sisteme de operare suportate	Windows® 2000, Windows Server 2003, Windows XP, Linux®, Sun™ Solaris™, Mac® OS, VMware ESX
Copii instantanee de date	Minim 100000
Functii de management al echipamentului	diagnostic LED, SNMP, telnet, SSH, HTTP, Web (SSL), host scripting, alerte pe e-mail

Funcții de securitate	SecureAdmin, IPSec, autentificare CHAP, acces pe baza de roluri administrative (RBAC)
Sursa de alimentare	Minim 2 surse redundante cu alimentare 200 la 240VAC/1.9A cu un consum de maxim 600W
Ventilatoare	Ventilatoare redundante

3.6.2 Alte echipamente

3.6.2.1 Firewall

Descriere generala	Echipament integrat de protectie in retea cu capabilitati de scanare antivirus, scanare antispam si prevenirea intruziunilor destinat folosirii ca o solutie de securitate unificata.
Specificatii hardware	<p>2 x interfete 10GbE SFP+</p> <p>8 x interfete 10/100/1000 Duale (RJ-45/SFP)</p> <p>12 x interfete 10/100/1000 Ethernet</p> <p>4 x interfete 10/100/1000 Ethernet cu bypass (functionare in pereche)</p> <p>2 x interfete 10/100/1000 Ethernet pentru Management</p> <p>2 x porturi USB</p> <p>1 x modul stocare intern 128 GB</p>
Performanta sistemului	<p>Firewall Throughput(pachete UDP 1514 byte): 20 Gbps</p> <p>Firewall Throughput(pachete UDP 512 byte): 20 Gbps</p> <p>Firewall Throughput(pachete UDP 64 byte): 20 Gbps</p> <p>Firewall Throughput(pachete pe secunda): 31 Mpps</p> <p>IPSec VPN Throughput(pachete 512 byte): 8 Gbps</p> <p>IPS Throughput: 3.6 Gbps</p> <p>Antivirus Throughput(flow-based): 2.1 Gbps</p>

	<p>Antivirus Throughput(proxy-based): 1.7 Gbps</p> <p>Tunele IPSec VPN (gateway to gateway) concurente: 10000</p> <p>Tunele IPSec VPN (client to gateway) concurente: 50000</p> <p>Useri SSL-VPN: 3000</p> <p>SSL-VPN Throughput: 350 Mbps</p> <p>Concurrent session(TCP): 7 Milioane</p> <p>New Session/Sec(TCP): 190000</p> <p>Policies(Maxim): 100000</p> <p>Domenii virtuale: 100</p> <p>Configuratii redundante posibile: Activ/Activ, Activ/Pasiv, Cluster</p> <p>Unlimited Users Licences</p>
Parametrii echipament	<p>Alimentare alternativa 100-240V, 50-60Hz</p> <p>2 x surse de alimentare redundante Hot-swappable</p>
Protocoale si standarde	<p>Servicii de Retea</p> <p>Rutare/Retea: Suport WAN multiplu</p> <p>Suport PPPoE</p> <p>Client/Server DHCP</p> <p>Policy-based routing</p> <p>Rutare dinamica IPv4/IPv6-RIP,OSPF,BGP,Multicast(IPv4)</p> <p>Suport multi-zone</p> <p>Rutare intre zonele de securitate</p> <p>VLAN Tagging(802.1q)</p> <p>Rutare intre VLAN-uri</p> <p>Multi-link aggregation(802.3ad)</p> <p>Suport IPv6 (Firewall,DNS,Transparent,SIP,rutare dinamica)</p> <p>Traffic</p> <p>Shaping: Policy-based</p>

	<p>Suport DiffServ</p> <p>Banda Garantata/Maxima/Prioritara</p> <p>Shaping per-IP,per-Account, per aplicatie</p> <p>Domenii</p> <p>Virtuale: Domenii Firewall/Rutare separate</p> <p style="padding-left: 40px;">Politici de securitate per domeniu</p> <p style="padding-left: 40px;">Interfete VLAN separate</p> <p>High Availability:</p> <p style="padding-left: 40px;">Funcționare Activ/Activ, Activ/Pasiv</p> <p>Statefull Failover</p> <p>Link status monitor</p> <p style="padding-left: 40px;">Link failover</p> <p>Server Load Balancing</p> <p>Servicii de Securitate</p> <p>Firewall: NAT,PAT,Transparent</p> <p style="padding-left: 40px;">Rutare dinamica-RIP,OSPF,BGP,Multicast</p> <p>Policy-based NAT</p> <p>Domenii Virtuale (NAT/Transparent)</p> <p style="padding-left: 40px;">VLAN Tagging(802.1q)</p> <p>SIP/H.323/SCCP NAT Traversal</p> <p>Profile granulare de protectie per-policy</p> <p style="padding-left: 40px;">Suport proxy explicit, optimizare WAN, caching</p> <p style="padding-left: 40px;">Suport IPv6</p> <p>VPN: PPTP,IPSec,SSL</p> <p>Suport criptare DES,3DES,AES</p> <p>Autentificare SHA-1 / MD5</p> <p>PPTP,L2TP,VPN Client pass through</p>
--	---

	<p>Suport VPN "Hub and Spoke"</p> <p>Autentificare IKE cu Certificate(v1 si v2)</p> <p>IPSec NAT Traversal</p> <p>Prevenirea Intruziunilor Suport Anomalii de protocoale</p> <p>Suport Semnaturi definite de utilizator</p> <p>Suport IPv6</p> <p>Antivirus Protecție anti-malware (virus, troian, worm, spyware)</p> <p>Protocoale: HTTP/HTTPS; POP/POP3S; SMTP/SMTPS; IMAP/IMAPS, IM (AIM, ICQ, Yahoo, MSN)</p> <p>Blocare fisierelor in functie de tip sau dimensiune</p> <p>Suport Ipv6</p> <p>Antispam SMTP/SMTPS;IMAP/IMAPS;POP/POPS</p> <p>Suport RBL/ORDBL</p> <p>Inspecție header MIME, filtrare dupa cuvinte/expresii si black/white list</p> <p>Update-uri automate și în timp real.</p>
Management	<p>Administrare: Consola, Telnet, SSH, HTTP/HTTPS,CLI</p> <p>Utilizatori/Administratori cu drepturi configurabile</p> <p>Syslog,SNMP,log-uri interne,grafice,notificari email</p> <p>Autentificare: Baza de date locala</p> <p>Integrare Active Directory</p> <p>Integrare LDAP/Radius/TACACS+</p> <p>IP/MAC address binding</p>
Software	<p>Echipamentul sa permita prin achizitia unor licente suplimentare activarea si actualizarea serviciilor Antivirus, Antispam, Prevenirea Intruziunilor,etc. Aceste functii trebuie sa fie asigurate de echipament fara a mai necesita vreun modul hardware suplimentar.</p>

Service si garantie	Garantie: minim 3 ani Update software gratuit: minim 3 ani
---------------------	---

3.6.2.2 Notebook – (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimele:

Procesor	x_86 cu 4-core sau echivalent, frecventa minim 2.4 GHz
Memorie RAM	Minim 4GB
Placa Video	Dedicata, Minim 1GB
Hard disk	Minim 500GB
Unitate optica	DVD RW
Camera WEB	Da, Minim 1,3MP
Display	LCD LED, minim 15 inch
Audio	Difuzoare stereo incorporate
Comunicatii	Retea: 10/100/1000 Wireless:WiFi 802.11n; Bluetooth
I/O (Input/Output) Porturi si Sloturi	VGA: 1 Microfon: 1 RJ-45: 1 USB 3.0: 2 Iesire audio: 1 HDMI: 1
Sistem de operare	Da
Garantie	Minim 2 ani, locala

Altele	Geanta notebook de dimensiuni adecvate produsului achizitionat Mouse fara fir conectivitate Bluetooth Alimentator notebook
---------------	--

3.6.2.3 Multifunctionala - (1 bucata)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minime:

Format	A4
Functii disponibile	Copiere, imprimare, scanare, fax
Tehnologie	Laser
Mod tiparire	Color
Duplex	Da
Interfata	USB, retea
ADF	Da
Medii printare	A4, A5,
Viteza de copiere color	8 / minut
Viteza de copiere alb negru	18 / minut
Rezolutie copiere	Minim 600 dpi
Viteza de printare color	21 / minut
Viteza de printare alb negru	21 / minut
Rezolutie printare	Minim 600x600 dpi
Rezolutie scanner	Minim 600x600 dpi
Alimentare hartie	Minim 250 coli
Capacitate memorie	Minim 256 MB

3.6.2.4 Flipchart – (1 bucata)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minime:

Suprafata	Magnetica
Inaltime	Minima ajustabila 1500mm, maxima 2000mm
Dimensiuni suprafata de scris	Minim 1000 x 500 mm
Altele	Sa fie dotat cu role pentru o manevrabilitate usoara Suport pentru instrumentele de scris Brate laterale pentru afisarea a doua pagini in plus

3.6.2.5 Desktop “All in One” – (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minime:

Tip ecran	LED
Diagonala	Minim 23 inch
Rezolutie	Minim 1920x1080
Procesor	x_86 cu 4-core sau echivalent, frecventa minim 2.5 (GHz)
Sunet integrat	Da
Retea integrata	Da
Capacitate RAM	Minim 4GB
Capacitate HDD	Minim 500GB
Tip placa video	Dedicata
Capacitate memorie	Minim 1024 MB
Difuzoare	Da

Microfon	Da
Tip unitate optica	DVD-RW
Webcam	Da
Bluetooth	Da
Retea	Da
Wireless	Da
USB 2.0	Minim 4
Iesire audio	Da
Intrare microfon	Da
Sistem de operare	Da
Accesorii	Tastatura fara fir conectivitate Bluetooth Mouse Mouse fara fir conectivitate Bluetooth

3.6.2.6 Tableta electronica - (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minime:

Frecventa Procesor	Minim 1Ghz
Tehnologie display	Capacitive Multi-Touch sau echivalent
Diagonala	Minim 9.7 inch
Rezolutie	Minim 1024 x 768
Memorie Flash integrata:	Minim 16 GB
Audio	Difuzor integrat
Camera WEB	In spate: Minim 3 MP In fata: Minim 0.3 MP
Iesire audio	Minim 1 x 3.5 mm

Bluetooth	Da
Wireless	802.11 b/g/n sau echivalent
3G	Da
Baterie	Li-Polymer sau echivalent
Autonomie de lucru	Minim 9 ore
Sistem de operare	Da

3.6.2.7 Televizor cu suport mobil – (1 bucata)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimele:

Tehnologie	LED
3D	Da
Iesire sunet (RMS)	Minim 2 x 10 W
Diagonala ecran (cm)	Minim 162
Calitate imagine	Full HD
Rezolutie	Minim 1920 x 1080
Aspect imagine	16:9
Tuner digital	DVB-T/C/S2
Conexiune retea	RJ45 Wireless
Intrare USB 2.0	Minim 3
Intrare video composite	Minim 1

Intrari Scart (RGB)	Minim
Porturi HDMI	Minim 3
lesire audio digitala (optica)	Minim 1
Conexiuni	HDMI SCART Slot CI+
Intrari component	Minim 1
Stand mobil	Da

3.6.2.8 Hard Disk Drive Extern - (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimale:

Capacitate:	Minim 2 TB
Interfata:	USB 2.0 USB 3.0
Altele	Plug-and-play Minim 5 Gb/sec in USB 3.0 Minim 480 Mb/sec in USB 2.0
Sisteme de operare	Microsoft Windows 7 Microsoft Windows Vista Microsoft Windows XP
Format	Minim 2.5"

3.6.2.9 Memory Stick USB – (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimele:

Capacitate (GB):	Minim 64
Interfata	USB 2.0 USB 3.0
Rata de transfer la citire (MB/s):	225 (USB 3.0) 30 (USB 2.0)
Rata de transfer la scriere (MB/s):	135 (USB 3.0) 30 (USB 2.0)
Altele	Carcasa din metal sau cauciuc

3.6.2.10 Distrugator de documente – (1 bucata)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimele:

Capacitate de taiere	Minim 10 coli
Dimensiuni taiere	Minim 2 x 8 mm
Volum cos	Minim 28 L
Nivel zgomot (dB)	Maxim 44
Viteza (m/min)	Minim 3

4 CERINTE PRIVIND SERVICIILE DE PROMOVARE SI PUBLICITATE

4.1 Plan de informare și publicitate

Cerinte:

- Prestatorul va realiza un plan de informare si publicitate a proiectului ce va contine o metodologie de specialitate in ceea ce priveste diseminarea/comunicarea informatiilor cu privire la proiect
- Prestatorul va realiza un plan de informare si publicitate a proiectului ce va contine un grafic de realizare a activitatilor de informare si publicitate.
- Planul de informare si publicitate va fi livrat Autoritatii Contractante in termen de 7 zile lucratoare de la data semnarii contractului de prestari servicii.

4.2 Organizare evenimente de promovare a proiectului

Livrabile:

- organizare eveniment de lansare a proiectului
- organizare eveniment de diseminare a rezultatelor proiectului

Prestatorul va realiza urmatoarele activitati:

- **Elaborarea agendei evenimentului și a invitațiilor de participare**

Cerinte:

- Agenda evenimentului va cuprinde: discuții asupra obiectivelor proiectului/rezultatele proiectului, sursele de finantare, beneficiile implementarii proiectului.
- Vorbitorii vor fi desemnati de autoritatea contractanta si vor fi comunicati prestatorului cu cel puțin 10 zile lucratoare inainte de data de derulare a evenimentului.
- Agenda evenimentului si textul invitatiei de participare vor fi elaborate cu cel puțin 10 zile lucratoare inainte de data de derulare a evenimentului si vor fi transmise spre aprobare autoritatii contractante.

- **Transmiterea invitatiilor**

Cerinte:

- Lista cu potentialii participanti va fi comunicata de autoritatea contractanta prestatorului cu cel putin 10 zile lucratoare inainte de data de derulare a evenimentului.
- Invitatiile de participare vor fi transmise potentialilor participanti cu cel putin 5 zile lucratoare inainte de data de derulare a evenimentului printr-o modalitate care sa asigure primirea acestora.
- Lista de invitati confirmati va fi transmisa de prestator autoritatii contractante cu cel putin 2 zile lucratoare inainte de data de derulare a evenimentului.
- **Desfășurarea evenimentului**

Cerinte:

- Organizarea unei conferinte de lansare (luna 5 de desfasurare a proiectului) si a unei conferinte de incheiere a proiectului (luna 12 de desfasurare a proiectului) cu urmatoarele caracteristici:
 - locul de derulare: Bucuresti
 - program: 10.00 – 12.00
 - numar de participanti: 50
 - sala de conferinte care sa permita prezenta a cel putin 50 de persoane
 - dotari: videoproiector cu ecran de proiectie, telecomanda, pointer laser, laptop, flipchart, foi de flipchart, markere – negru, verde, albastru, rosu
 - aer conditionat reglabil din sala
 - o pauza de cafea pentru 50 de persoane care sa contina: cafea, ceai, apa minerala, apa plata.
 - o persoana cu atributii de asistent de eveniment care sa realizeze inregistrarea participantilor si distribuirea materialelor de prezentare precum si sa solutioneze de indata orice problema administrativa sau tehnica legata de sala de conferinte si dotarile acesteia.

Conferinta va fi vizibila prin afise pozitionate in cel putin urmatoarele locuri: unul la intrarea in cladirea ce gazduieste conferinta, unul pe parcursul drumului parcurs de participanti de la intrare in cladire pana la sala unde are loc conferinta si unul in apropierea intrarii in sala in care se deruleaza conferinta. In sala in care are loc conferinta va fi instalat banner-ul de tip roll-up, in apropierea prezidiului.

Prestatorul va realiza un raport al conferintei in cel mult 5 zile lucratoare de la finalizare, ce va contine cel putin:

- agenda
- lista de participanti semnata de fiecare dintre acestia
- fotografiile de la conferinta, ce vor surprinde si elementele de identitate vizuala ale proiectului.

4.3 Editarea, producția, tipărirea/multiplicarea, inscripționarea și distribuția de materiale promoționale

Prestatorul va realiza următoarele activități:

- **Elaborarea conținutului materialelor promoționale: pixuri, calendare, agende, afise, banner, autocolante**

Cerinte:

- Toate materialele vor fi elaborate în conformitate cu Manualul de identitate vizuală pentru instrumentele structurale 2007-2013 în România (obiectivul Convergență).
 - Materialele tiparite vor conține date referitoare la obiectivele proiectului, sursele de finanțare, beneficiile și rezultatele implementării.
 - Toate mostrele de materiale promoționale vor fi elaborate de către prestator și transmise autorității contractante cu cel puțin 10 zile lucrătoare înainte de termenul pentru trimiterea acestora în producție. Autoritatea contractantă va comunica observațiile în termen de cel mult 48 de ore de la primirea propunerilor de materiale. Textul materialelor tiparite (cum ar fi pliante, afise, calendare) va fi furnizat de către autoritatea contractantă.
 - Un număr de 5 exemplare din fiecare material vor fi transmise autorității contractante pentru a fi incluse în rapoartele către finanțator.
 - Materialele promoționale vor fi livrate de către prestator la sediul autorității contractante cu cel puțin 5 zile lucrătoare înainte de data desfășurării conferinței de lansare a proiectului.
- **Tipărirea/multiplicarea, inscripționarea și distribuția materialelor promoționale**

Cerinte:

Nr.crt.	Denumire	UM	Numar de unitati
1.	Pliante: format inchis: 100 x 210 mm, format deschis: 200 x 210 mm, hârtie: dublucretat lucios 130g, culori: 4+4	buc	100

Nr.crt.	Denumire	UM	Numar de unitati
2.	Banner rollup , format 0,8 x 2 m, 4+0 print + suport aluminiu.	buc	1
3.	Afise format A3 cm, suport 150 g/mp lucios, print 4+0, autoadeziv pe spate, în colțuri.	buc	30
4.	Pixuri din plastic rezistent, personalizat. Mină pix: albastru.	buc	100
5.	Agende format închis A5 , coperta 300 g/mp plastifiată mat față – verso, interior 135 g/mp mat, tipar copertă 4+4, tipar interior 4+4, 100 pag. interior, finisări: spirala.	buc	100
6.	Calendar format 50 x 70 cm, suport 150 g/mp lucios, print 4+0.	buc	30
7.	Autocolante plastificate format 90 x 50 mm (lungime x latime), color.	buc	100

4.4 Elaborare comunicate de presa

Cerinte:

- Prestatorul va elabora 2 comunicate de presa privind implementarea proiectului, astfel:
 - 1 comunicat de presa privind inceperea proiectului
 - 1 comunicat de presa la inchiderea proiectului cu mentionarea rezultatelor obtinute
- Comunicatele de presa vor fi formulate de catre prestator si transmise autoritatii contractante spre aprobare cu cel putin 3 zile lucratoare inainte de data la care sunt programate a fi distribuite. Autoritatea Contractanta va transmite aprobarea insotita de eventualele observatii in cel mult 1 zi lucratoare de la primirea propunerii de comunicat de presa.
- Prestatorul va suporta difuzarea celor 2 comunicate de presa catre minim 3 fluxuri de presa cu diseminare la nivel national.

4.5 Realizare pagina Web si publicare anunturi

Cerinte:

- Prestatorul va realiza o pagina web dedicata proiectului ce va contine informatii despre proiect, anunturi de presa, comunicate si legaturi utile catre website-ul

Ministerului Comunicațiilor și Societății Informaționale, www.fonduri-ue.ro, etc. Pagina Web va fi gazduita ca subdomeniu la adresa www.mcsi.ro.

- Prestatorul va redacta anunturi cuprinzand informatii despre proiect si le va trimite autoritatii contractante in vederea publicarii pe pagina web a proiectului respectiv pagina web www.mcsi.ro.
- Anunturile vor cuprinde informatii privind stadiul implementarii proiectului, beneficiile proiectului si despre sursa de finantare.
- Prestatorul va redacta si publica anunturi informative pe pagina web a proiectului, pagina web a MCSI astfel incat sa fie publicat cel putin unul in fiecare luna de implementare a contractului.

5 CERINTE PRIVIND SERVICIILE DE MANAGEMENT DE PROIECT

Ofertantul va asigura Ministerului Comunicațiilor și Societății Informaționale suportul necesar în vederea implementării în bune condiții a proiectului și elaborarea tuturor documentelor de raportare solicitate de către OIPSI pe perioada implementării acestui proiect.

Activitățile principale ce urmează a fi prestate de către Ofertant constau în:

1. Inițializarea proiectului
 - a. Organizarea ședințelor pentru demararea proiectului
 - b. Clarificarea rolurilor și responsabilităților
2. Planificarea proiectului
3. Monitorizare și control
 - a. Colectarea, înregistrarea și raportarea periodică a informațiilor referitoare la progresul proiectului
 - b. Analize trimestriale cu privire la starea implementării proiectului
 - c. Determinarea riscurilor în realizarea proiectului și realizarea de recomandări pentru tratarea acestora
 - d. Realizarea managementului documentației proiectului
 - e. Monitorizarea și controlul costurilor, raportare financiară
 - f. Coordonarea implementării proiectului conform planului de lucru
 - g. Verificarea realizării fiecărei subactivități și activități în parte și acordarea acceptanțelor parțiale către furnizori;
4. Comunicare
 - a. Comunicarea permanentă cu echipa implementatorului proiectului în vederea monitorizării progreselor realizate;
 - b. Raportarea periodică asupra progreselor realizate în implementarea proiectului, către responsabilul de proiect din partea Ministerului Comunicațiilor și Societății Informaționale;
 - c. Menținerea contactului permanent cu Organismul Intermediar pentru Promovarea Societății Informaționale (OIPSI);

5. Managementul calității și schimbării

- a. Monitorizarea calității serviciilor de implementare a proiectului;
- b. Validarea calității activităților de implementare a proiectului
- c. Managementul activităților de acceptanță a livrabilelor proiectului

Aceste activități trebuie considerate ca fiind cerințe minime, iar dacă alte activități relaționate sunt necesare în vederea realizării obiectivelor activității de management de proiect, acestea vor face parte din responsabilitatea Prestatorului.

Prestatorul va îndeplini toate sarcinile de raportare ale Beneficiarului față de Organismul Intermediar, în conformitate cu prevederile Contractului de Finanțare.

Prestatorul va fi responsabil din punct de vedere tehnic și financiar față de Autoritatea Contractantă.

Următoarele activități de management al proiectului vor fi realizate de către Ofertant:

- elaborarea rapoartelor de progres
- suport pentru fundamentarea și elaborarea Cererilor de rambursare
- suport pentru managementul financiar al proiectului
- asigurarea suportului privind informarea și publicitatea pentru proiectul ce urmează a fi implementat
- elaborarea sistemului de arhivare a documentației proiectului.

Prin personalul pus la dispoziție de către furnizorul selecționat în urma acestei proceduri de achiziție, Ofertantul va realiza următoarele activități generale:

Management de proiect

- Monitorizare activitate management de proiect extern – derularea proiectului va fi monitorizată de către o echipă de monitorizare din cadrul Ministerului Comunicatiilor si Societatii Informatiionale.
- Întocmirea planului de lucru – echipa de management al proiectului va realiza și agreea un plan de lucru cu toate părțile implicate în proiect
- Raportare – activitatea de întocmire a rapoartelor se întinde pe tot parcursul proiectului.
- Management financiar-contabil – toate cheltuielile aferente proiectului vor fi urmărite cu atenție, pentru a se asigura respectarea tuturor obligațiilor și cerințelor contractuale.

Activitatea de management reprezintă o activitate continuă pe tot parcursul proiectului

Totodată, managementul proiectului cuprinde activitățile:

- Planificarea activităților proiectului pentru încadrarea în graficul de implementare aprobat prin Contractul de Finanțare
- Monitorizarea tuturor activităților proiectului, derulate atât de către echipa de proiect a Beneficiarului cât și de către Furnizor
- Monitorizarea respectării de către furnizorul tehnic a angajamentelor asumate prin contract
- Managementul riscurilor (identificare, analiză, planificare, urmărire) prin întreținerea unui Registru de Riscuri și planificarea măsurilor de prevenire și reducere
- Managementul calității prin întreținerea unui Registru de Calitate în care să se înscrie toate problemele apărute pe durata derulării proiectului (în cadrul testelor de acceptanță) și prin urmărirea rezolvării acestor probleme
- Managementul schimbării – pregătirea și aplicarea unei proceduri de tratare a cererilor de schimbare prin care să se asigure introducerea controlată a schimbărilor în cadrul ciclului de analiză-proiectare-dezvoltare-implementare-testare-acceptanță.

Management Financiar

- Consultantul va furniza suport în vederea înregistrării cheltuielilor proiectului
- Consultantul va întocmi cererile de rambursare către Finanțator, astfel:

Cerere de rambursare nr.	Activitate/ subactivitate	Data depunerii (ziua x, luna y, anul z de la semnarea Contractului de Finanțare)
Cerere de rambursare nr. 1	Managementul de proiect/ Implementarea soluției/ Instruirea utilizatorilor/Informare si publicitate/ Auditarea proiectului	Până la ultima zi, luna 6, anul 1 de la semnarea contractului
Cerere de rambursare nr. 2	Managementul de proiect/ Implementarea soluției/ Instruirea utilizatorilor/Informare si	Până la ultima zi, luna 9, anul 1 de la semnarea contractului

	publicitate	
Cerere de rambursare nr. 3	Managementul de proiect/ Implementarea soluției/ Instruirea utilizatorilor/ Informare și publicitate/ Auditarea proiectului	Până la ultima zi, luna 12, anul 1 de la semnarea contractului
Total asistență financiară nerambursabilă		

Raportare către Finanțator

- Consultantul va elabora Rapoartele Tehnice periodice de progres
- Consultantul va elabora rapoartele lunare de stare cu privire la derularea activităților proiectului tehnic
- Arhivarea documentelor – are drept scop păstrarea și arhivarea documentelor generate în cadrul proiectului, pentru a asigura o pistă adecvată de audit.

Monitorizarea activităților de management al proiectului

Monitorizarea serviciilor de management al proiectului va fi realizată de o echipă de monitorizare din partea Ministerului Comunicatiilor și Societății Informationale pe baza rapoartelor săptămânale transmise de către Prestatorul serviciilor de management de proiect.

6 RESURSE

6.1 Personal și instruire

6.1.1 Managementul proiectului, personal și instruire

6.1.1.1 Managementul proiectului

Managementul de proiect reprezintă procesul de coordonare, organizare și gestionare a activităților interdependente și a resurselor alocate, pentru a asigura atingerea obiectivelor stabilite la standardele de calitate solicitate, în condițiile existenței unor constrângeri referitoare la timp, resurse și costuri.

Metodologia de management de proiect care va fi folosită pentru finalizarea cu succes a tuturor activităților propuse în prezentul proiect are următoarele componente:

I. Activități generale de management de proiect

- Planificare și organizare
- Coordonare și monitorizare
- Control și raportare
- Activități specifice proiectelor europene:
 - management financiar
 - asigurarea vizibilității proiectului în conformitate cu regulile de identitate vizuală prevăzute de Manualul de identitate vizuală publicat pe website-ul O.I.P.S.I
 - asigurarea calității proiectului urmărește realizarea unor sisteme eficiente de verificare și păstrare a documentațiilor tehnice și financiare ale proiectului, care să confere siguranță și un acces facil la aceste documentații, în cazul vizitelor de monitorizare sau al auditurilor parțiale și finale.

6.1.1.2 Personalul și echipa tehnică a proiectului

6.1.1.3 Necesitatea contractării managementului de proiect

Ministerul Comunicațiilor și Societății Informaționale va contracta serviciile de management al proiectului, întrucât instituția dorește să beneficieze de o expertiză superioară în domeniul managementului proiectelor finanțate prin fonduri europene.

Astfel va fi asigurat suportul pentru Ministerul Comunicațiilor și Societății Informaționale în vederea implementării în bune condiții a proiectului și elaborarea tuturor documentelor de raportare solicitate de către OIPSI pe perioada implementării acestui proiect. Implementarea în cele mai bune condiții va fi asigurată de către Ministerul Comunicațiilor și Societății Informaționale prin furnizarea unei echipe de implementare, prezentată mai sus.

Activitățile de management de proiect ce urmează a fi contractate

Următoarele activități de management al proiectului vor fi contractate:

- elaborarea rapoartelor de progres
- suport pentru fundamentarea și elaborarea Cererilor de rambursare
- suport pentru managementul financiar al proiectului
- asigurarea suportului privind informarea și publicitatea pentru proiectul ce urmează a fi implementat
- elaborarea sistemului de arhivare a documentației proiectului.

Metodologia de management de proiect

Concret, activitățile specifice proiectelor finanțate din fonduri europene vor fi realizate astfel:

I. Achiziții

În procesul de desfășurare a procedurilor de achiziții publice, echipa de achiziții va utiliza următorul model:

Valoare Contract (exclusiv TVA)	Tip contract	Proceduri de achiziție			Referință legislativă
		Achiziție directă	Cerere de ofertă	Licitație deschisă	
	Servicii (S) Bunuri (B)	< 15.000 Euro sau echivalent în lei	< 125.000 Euro sau echivalent în lei	≥125.000 Euro sau echivalent în lei	Art. 19, art.20(1) și art.124 din O.U.G. nr. 34/2006, cu modificările și completările ulterioare

Procedurile menționate mai sus se vor derula cu stricta respectare a legislației în vigoare.

Input:

- informații privind sistemele informatice existente
- cerințe de asistență tehnică
- analiza de nevoi și studiu de fezabilitate
- caiete de sarcini și documentații de atribuire pentru servicii și bunuri

Output:

- Contracte de servicii și bunuri.

II. Management financiar

Pentru o bună gestionare a bugetului alocat proiectului, până la rambursarea sumelor solicitate, echipa consultantului va elabora un registru de cheltuieli, pentru înscrierea cronologică a tuturor cheltuielilor făcute, defalcate în eligibile și neeligibile, precum și a detaliilor documentelor justificative și a datelor plăților efective.

Etapa de verificare a cheltuielilor are ca scop asigurarea conformității tuturor cheltuielilor efectuate în cadrul proiectului cu prevederile Ghidului Solicitantului, contractului de finanțare și legislației în vigoare. Totodată vor fi elaborate cererile de rambursare, care vor însoți rapoartele de progres și care vor fi înaintate spre aprobare către O.I.P.S.I.

Input:

- Documente contabile (facturi, ordine de plată, etc.)
- Planul de cheltuieli
- Bugetul proiectului

Output:

- Registrul de cheltuieli
- Cererile de rambursare

III. Elaborarea rapoartelor de progres și a cererilor de rambursare

Echipa Consultantului selectat va oferi suport pentru Ministerul Comunicațiilor și Societății Informaționale în vederea realizării rapoartelor de progres stabilite prin contractul de finanțare. Astfel rapoartele de progres vor fi elaborate de către Managerul de proiect și înaintate către Coordonatorul de proiect din partea Ministerului Comunicațiilor și Societății Informaționale, care va verifica și semna rapoartele mai sus-menționate. Rapoartele de progres se vor baza pe informațiile din rapoartele de activitate transmise lunar de către Managerul de proiect și discutate în cadrul întâlnirilor de monitorizare.

Aceste rapoarte vor respecta întocmai cerințele specificate în Ghidul Solicitantului și în contractul de finanțare semnat cu O.I.P.S.I. și vor fi depuse la O.I.P.S.I. la termenele stabilite conform contractului, împreună cu toate celelalte documente solicitate în mod expres prin contractul de finanțare.

Cererile de rambursare, care vor fi atașate rapoartelor de progres, vor fi elaborate de către Managerul de proiect cu sprijinul Responsabilului Financiar, iar dosarul de rambursare va fi pregătit în conformitate cu cerințele specificate în contract și va conține toate documentele justificative necesare verificării eligibilității cheltuielilor efectuate și efectuării plății.

Input:

- Bugetul proiectului, registrul de cheltuieli, documente contabile – în copie certificată
- Contractul de finanțare
- Rapoartele de activitate ale Furnizorilor de servicii și bunuri

Output:

- Rapoarte de progres
- Cereri de rambursare

IV. Arhivarea documentelor

Conform regulamentelor comunitare circuitul auditului (pista de audit) reprezintă stabilirea fluxurilor informațiilor, atribuțiile și responsabilitățile referitoare la acestea, precum și arhivarea documentației justificative complete, pentru toate stadiile desfășurării unei acțiuni, care să permită totodată reconstituirea operațiunilor de la suma totală până la detalii individuale și invers.

Pista de audit este deci o înregistrare cronologică a activităților din proiect pentru a permite reconstrucția și examinarea succesiunii de evenimente și/sau schimbări.

Solicitantul va pregăti și asigura o pistă de audit adecvată prin măsuri de păstrare și arhivare a documentelor astfel încât acestea să nu fie alterate de factorul uman și de timp.

Astfel, cu sprijinul Consultantului, Ministerul Comunicațiilor și Societății Informaționale va întreprinde următoarele măsuri:

- exemplarele originale ale facturilor și documentelor care atestă efectuarea plăților vor fi păstrate de către Ministerul Comunicațiilor și Societății Informaționale, la locația proiectului, împreună cu o copie certificată, atât pe suport de hârtie cât și electronic (CD/DVD etc.).
- documentele elaborate în cadrul proiectului vor fi păstrate astfel: 1 exemplar original și 1 copie pe suport hârtie cât și în variantă electronică.
- rapoartele, cererile de rambursare și alte documente oficiale solicitate de către O.I.P.S.I vor fi elaborate într-un exemplar original și numărul de exemplare - copii stabilite prin contractul de finanțare, care vor fi predate O.I.P.S.I., câte o copie certificată a acestora păstrându-se la sediul proiectului.
- arhivarea se va face la finalizarea proiectului, dosarul complet cu documentele în original va fi păstrat într-un spațiu protejat, împreună cu un CD/DVD cuprinzând toate documentele scanate, acesta rămânând la locația proiectului pe perioada legală de arhivare și păstrare (5 ani post-implementare).

Input:

- bugetul proiectului și registrul de cheltuieli, documente contabile – în original și în copie certificată
- contractul de finanțare
- rapoarte de progres și cereri de rambursare, alte documente realizate în cadrul proiectului
- procedura de arhivare

Output:

- dosarele / cutia de arhivă, corect inscripționate și păstrate
- copia în suport electronic a arhivei hard-copy a proiectului

V. Asigurarea vizibilității proiectului

Această activitate are o deosebită importanță în diseminarea oportunităților de finanțare puse la dispoziția administrației publice pentru realizarea de sisteme informatice în vederea îmbunătățirii calităților serviciilor către cetățeni și mediul de afaceri. Activitatea de informare și publicitate va respecta reglementările Uniunii Europene, fiind pregătită de către Ministerul Comunicațiilor și Societății Informaționale, împreună cu consultantul selectat, și derulându-se pe tot parcursul proiectului.

Input:

- Planul de informare și publicitate, informații privind proiectul

Output:

- Anunțuri de presă și comunicate pe website-ul Ministerului Comunicațiilor și Societății Informaționale
- Evenimente de începere și finalizare a proiectului
- Pliante informative și postere

Cerințe minime solicitate pentru managementul de proiect

Consultantul pentru servicii de management de proiect care urmează a fi contractat va îndeplini următoarele condiții minime:

Să aibă specialiști în următoarele domenii:

- Managementul proiectului
- Fonduri nerambursabile
- Financiar
- Informare și Publicitate

- Formare / Instruire în managementul de proiect
- IT&C

I. Manager de proiect

Sarcini și responsabilități

Managerul de proiect raportează direct Coordonatorului de proiect și va asigura coordonarea echipei de consultanți și asistența către Coordonatorul de proiect desemnat de Ministerul Comunicațiilor și Societății Informaționale.

Responsabilități:

- Punct unic de contact în relația cu Beneficiarul
- monitorizarea implementării proiectului;
- elaborarea planului revizuit de activități și urmărirea respectării termenelor proiectului;
- elaborarea Rapoartelor de progres ce vor fi înaintate spre aprobarea Ministerului Comunicațiilor și Societății Informaționale;
- realizarea în colaborare cu responsabilul financiar a cererilor de rambursare;
- monitorizarea managementului financiar, incluzând verificarea cheltuielilor;
- identifică riscurile și modalitățile de atenuare/evitare a acestora;
- supraveghează îndeplinirea de către furnizor a obligațiilor asumate în conformitate cu contractul semnat.
- elaborarea sistemului de arhivare a documentelor și asigurarea pistei de audit aferente beneficiarului;
- coordonarea activităților de informare și publicitate aferente fiecărei etape a proiectului;
- asigurarea accesului ușor la documentația proiectului în vederea realizării auditurilor financiare și tehnice parțiale și finale.

II. Expert Fonduri Structurale

Responsabilități:

- întocmirea rapoartelor trimestriale de progres;
- întocmirea rapoartelor de progres care însoțesc cererea de rambursare;
- întocmirea Cererilor de rambursare;
- arhivarea dosarului final cu documentele generate în cadrul proiectului (5 ani post-implementare).

III. Responsabil Financiar

Responsabilități:

- elaborarea, împreună cu Coordonatorul de proiect din partea Ministerului Comunicațiilor și Societății Informaționale a planului de cheltuieli;
- verificarea disponibilității resurselor financiare necesare inițierii proiectului;
- asistență la elaborarea cererii de prefinanțare;
- verificarea cheltuielilor;
- verificarea aspectelor financiare ale contractelor de achiziții publice;
- elaborarea dosarului de rambursare;
- contribuție la elaborarea rapoartelor de progres;
- asigurarea accesului la documentația financiar-contabilă pentru auditorul extern;
- transfer de cunoștințe specifice de management financiar către echipa de implementare.

IV. Manager de proiect tehnic

Responsabilități:

- gestionarea implementării sistemului (componente hardware; software; securitate);
- coordonarea întregii echipe tehnice, cu alocarea sarcinilor pe fiecare membru al echipei;
- asigură o adresă de e-mail funcțională în scopul facilitării comunicării dintre echipa de proiect și beneficiar;
- asigură resurse pentru executarea serviciilor de implementare cuprinse în caietul de sarcini;
- menține și aplică managementul riscului și procedurile de asigurare a calității;
- întocmește toate rapoartele necesare conform cerințelor proiectului și /sau alte rapoarte cerute de către Managerul de Proiect.

V. Arhitect de soluție

Responsabilități:

- asigură proiectarea sistemului, începând din faza de analiză;
- asigură asistență și suport pentru pregătirea și validarea planurilor de calitate în vederea construirii și asigurării mentenanței sistemelor informatice
- raportează stadiului privind implementarea soluției către Managerul de proiect și către Coordonatorul de proiect din partea Ministerului Comunicațiilor și Societății Informaționale.

VI. Arhitect infrastructură hardware și comunicații

Responsabilități:

- evaluarea necesităților infrastructurii hardware și de comunicații, precum și implementarea părții de comunicații din proiect;
- raportarea stadiului privind implementarea soluției către Managerul de proiect și către Coordonatorul de proiect din partea Ministerului Comunicațiilor și Societății Informaționale.

VII. Expert analist de business

Responsabilități:

- realizează studii de consultanță cu privire la aspectele organizatorice în dezvoltarea TIC a sistemelor informatice;
- analizează și definește procesele de business (work-flow) și elaborează specificațiile de proces;
- coordonează analiza cerințelor de schimb de date cu toate structurile implicate și elaborează raportul diagnostic.

VIII. Specialist în informare și publicitate

Responsabilități:

- asigură informarea și publicitatea proiectului conform normelor de vizibilitate ale U.E;
- realizează comunicatele / anunțurile de presă;
- organizează evenimentele de informare din cadrul proiectului;
- realizează materiale promoționale.

IX. Specialist documentare tehnică și asigurarea calității

Responsabilități:

- pregătește întreaga documentație suport aferentă implementării și transferului de know-how către Beneficiar;
- urmărește implementarea metodologiilor de dezvoltare / instalare / testare / validare software;
- urmărește asigurarea calității în procesul de dezvoltare / instalare / testare / validare software;

X. Specialist în formare/instruire profesională

Responsabilități:

- Asigură formarea/instruirea în managementul de proiect;

Procedura de monitorizare utilizată de echipa de management

Procesul de monitorizare presupune obținerea informațiilor care să permită cunoașterea și înțelegerea stadiului proiectului la un moment dat, precum și tendințele de derulare a activităților incluse în proiect. Monitorizarea se poate face prin discuții cu personalul implicat în derularea proiectului, prin înregistrarea rezultatelor și a problemelor apărute, prin observarea activităților derulate. Monitorizarea permanentă a proiectului (se monitorizează activitățile, stadiul realizării planurilor, costurile, rezultatele proiectului) permite raportarea realizării acestuia, astfel obținându-se informațiile a căror procesare sprijină procesul de raportare.

Procedura de monitorizare a echipei de managementul proiectului contractate va include următoarele aspecte, fără a se limita doar la acestea:

- livrarea documentelor și rapoartelor necesare la timp, respectând cerințele impuse de Ghidul Solicitantului, Contractul de Finanțare și anexele sale, procedurile europene, legislația românească relevantă, planul de activități și termenele stabilite și înaintate spre aprobare Beneficiarului;
- activitățile de informare/publicitate (pentru serviciile de audit și informare și publicitate, dacă este cazul) sunt implementate conform planului de informare / publicitate și în conformitate cu Manualul de Identitate Vizuală;
- activitățile de achiziții sunt finalizate conform planificării proiectului, fiind implementate conform legislației românești în vigoare;
- rapoartele de progres pe baza rapoartelor de activitate ale proiectului, furnizate de către Consultant sunt aprobate de O.I.P.S.I.;
- cererile de rambursare înaintate către O.I.P.S.I. și elaborate cu asistența Managerului de proiect;
- calitatea și transparența sistemului de arhivare și înregistrare a informațiilor, vor fi monitorizate prin ușurința accesului specialiștilor care vor efectua auditurile tehnice și financiare parțiale și finale la documente, echipamente și soluții și tehnologii.

Calendarul aferent activităților de monitorizare este reprezentat în tabelul de mai jos:

Activități de monitorizare	Perioada de monitorizare (fiecare celulă reprezintă 1 lună calendaristică)											
	1	2	3	4	5	6	7	8	9	10	11	12
Ședințe de monitorizare												
Controlul costurilor												
Rapoarte lunare de activitate												
Rapoarte de progres												

Echipele consultantului, echipa internă a instituției și Coordonatorul de proiect se vor întâlni bilunar, în ședințe de câte două ore, pentru ca informațiile discutate să poată fi transmise, asimilate și puse în aplicare, într-un interval redus de timp. Ședințele de monitorizare bilunare se vor finaliza cu un proces verbal, care va fi semnat de toți participanții și care va fi arhivat, în original. Copii după procesul verbal vor fi transmise fiecărui participant și măsurile implementate vor fi discutate în deschiderea ședinței următoare.

Monitorizarea proiectului va urmări criteriile specificate mai sus și va fi consecventă pentru toți membrii echipei care urmează a implementa proiectul, atât reprezentanți ai Consultantului, cât și angajați ai instituției.

Această activitate se va baza în mod exclusiv pe date cuantificabile, pe indicatori și surse de verificare agreeți în prealabil, în ședința de începere a proiectului, când s-a fundamentat Planul de activități și planul de jaloane (milestones) ale proiectului, pe procesele verbale ale ședințelor de monitorizare precedente și pe baza termenelor și condițiilor prevăzute în alte documente elaborate în cadrul proiectului (planul de achiziții, planul de informare și publicitate, etc.).

Persoanele desemnate în echipa tehnică asigură configurarea sistemului informatic în funcție de soluțiile adoptate, le integrează în fluxul activităților Administrației Centrale, definesc planul testului de acceptanță al sistemului implementat, realizează testele pe date reale ale sistemului, sesizează eventuale disfuncțiuni, propun modalități de rezolvare, modalități de abordare a problemelor apărute. Se asigură că implementarea tehnică a sistemului să fie executată conform scopului propus.

Instruirea personalului care va utiliza/administra aplicația va fi realizată în cadrul a două activități de instruire specifică organizate în funcție de tipul de utilizatori (utilizatori și administratori). Astfel sunt propuse următoarele:

- instruirea dedicată utilizatori cheie (Ingineri suport sistem) ai soluției care urmează a fi achiziționată
- instruirea dedicată persoane care vor asigura administrarea soluției (Administratori sistem).

Se urmărește ca activitatea de instruire să cuprindă minimul de topici din modulele din tabelul următor:

Denumire curs	Durăță	Participanți	Tematică minimă necesară
Administrare baze de date 1	5 zile	Administratori sistem; Ingineri suport sistem	Instalarea și configurarea bazelor de date Crearea și administrarea conturilor de utilizator Backup and Recovery
Administrare baze de date 2	5 zile	Administratori sistem;	Crearea și gestionarea seturilor de backup și a copiilor imaginilor Recuperarea bazelor de date la un moment anterior în timp Refacerea bazei de date Depistarea blocurilor corupte și aplicarea măsurilor corespunzătoare pentru corectarea lor Utilizarea diverselor componente pentru monitorizarea și îmbunătățirea performanței bazelor de date Controlul folosirii resurselor bazelor de date Simplificarea sarcinilor de management Monitorizarea fișierelor log în

Denumire curs	Durată	Participanți	Tematică minimă necesară
			<p>scopul unei diagnoze corecte</p> <p>Setări dependente de limbă și teritoriu (globalizare) atât pentru sesiuni individuale, cât și la nivelul bazei de date</p> <p>Monitorizarea și gestionarea memoriei</p> <p>Gestionarea resurselor</p>
Construirea de rapoarte	5 zile	Ingineri suport sistem; Administratori de sistem	<p>Proiectarea și rularea rapoartelor</p> <p>Lucrul cu dezvoltatorul de rapoarte</p> <p>Crearea unui raport de printat</p> <p>Îmbunătățirea unui raport de bază de printat</p> <p>Administrarea modelelor de rapoarte</p> <p>Crearea unui raport web</p> <p>Îmbunătățirea rapoartelor utilizând modelul de date: interogări și grupuri</p> <p>Îmbunătățirea rapoartelor utilizând modelul de date: surse de date</p> <p>Îmbunătățirea rapoartelor utilizând modelul de date: crearea coloanelor</p> <p>Îmbunătățirea rapoartelor utilizând layout-ul paginii</p> <p>Controlul layout-ului paginii: proprietăți comune</p>

Denumire curs	Durață	Participanți	Tematică minimă necesară
			<p>Controlul layout-ului paginii: proprietăți specifice</p> <p>Raportare pe web</p> <p>Creșterea funcționalității utilizând XML</p> <p>Crearea și utilizarea parametrilor rapoartelor</p> <p>Încorporarea unui grafic într-un raport</p> <p>Îmbunătățirea rapoartelor matriciale</p> <p>Creșterea funcționalității</p> <p>Maximizarea performanței</p> <p>Principii de eficiență în construirea rapoartelor</p>
Construirea, testarea și exploatarea aplicațiilor Internet	5 zile	Ingineri de suport sistem	<p>Crearea modulelor formelor</p> <p>Lucrul cu blocuri de date și frame-uri</p> <p>Utilizarea paletii de proprietăți</p> <p>Utilizarea elementelor de intrare</p> <p>Utilizarea elementelor de tip „non-input”</p> <p>Crearea ferestrelor</p> <p>Elaborarea trigger-ilor</p> <p>Corectarea trigger-ilor</p> <p>Adăugarea de funcționalități item-ilor</p> <p>Interogarea trigger-ilor</p> <p>Validare</p> <p>Navigare</p>

Denumire curs	Durață	Participanți	Tematică minimă necesară
			<p>Procesarea tranzacțiilor</p> <p>Scrierea de cod flexibil</p> <p>Partajarea obiectelor și a codului</p> <p>Utilizarea instrumentelor pentru interacțiunea cu clientul</p> <p>Prezentarea aplicațiilor cu forme multiple</p>
Programare	5 zile	<p>Administratori de sistem;</p> <p>Ingineri suport sistem;</p>	<p>Declararea de identificatori</p> <p>Scrierea de instrucțiuni executabile</p> <p>Interacțiunea cu serverul</p> <p>Scrierea de structuri de control</p> <p>Lucrul cu tipuri de date compuse</p> <p>Folosirea de cursoare explicite</p> <p>Tratamentul excepțiilor</p> <p>Crearea de proceduri stocate</p> <p>Crearea de funcții stocate</p> <p>Exemplificarea de noi concepte privind pachetele de date</p> <p>Folosirea pachetelor în dezvoltarea de aplicații</p> <p>Managementul dependențelor</p> <p>Manipularea obiectelor mari</p> <p>Crearea triggerilor</p> <p>Aplicații bazate pe triggeri</p> <p>Înțelegerea și influențarea compilatorului</p>

6.2 Resurse materiale

Beneficiarul va pune la dispoziția echipei de proiectare a sistemului informatic următoarele:

- O sală în care se vor derula întâlnirile de lucru dintre echipele de proiect din partea integratorului și a beneficiarului;
- Un spațiu tehnic pentru amplasarea echipamentelor din cadrul proiectului;
- Beneficiarul nu va asigura resurse de tip tehnică de calcul pentru echipa de proiect a integratorului (stații de lucru, interconectare locală și/sau acces la internet sau rețele de voce);

7 MENTENANTA SI SUSTENABILITATE

7.1 Mentenanță

Mentenanța soluției informatice

Servicii de suport pentru soluția informatică

În timpul perioadei de garanție de 36 luni (pentru produsele hardware si software), Furnizorul va furniza pe baza acestui Service Level Agreement (SLA) următoarele servicii de suport:

- Servicii de Help Desk;
- Fault Management;
- Suport în caz de urgență;
- Rapoarte de deranjamente și corelarea erorilor;
- Subscripții software.

Problemele ridicate de Beneficiar vor fi înregistrate de către specialiști ai Furnizorului, în cadrul unei aplicații de tip HELPDESK.

Accesul la suportul telefonic, web sau e-mail va fi valabil șapte zile pe săptămână, 24 ore pe zi, 365 zile ale anului.

Clasificarea nivelelor de deranjament

Definițiile priorităților de deranjament sunt cele de mai jos:

Prioritate	Descrierea nivelului de prioritate
CRITIC	Deranjamente care afectează serviciile, cauzând nefuncționarea sistemelor sau blocarea funcțiilor importante de rețea sau subsisteme. Aceste deranjamente afectează în mod direct serviciile furnizate de elementele sau subsistemele de rețea, restricționează în mod semnificativ activitățile de operare în rețea sau clientul este afectat în totalitate.
MINOR	Problemele minore nu au un impact semnificativ în funcționarea sistemelor și nu afectează în mod direct serviciile clienților. Aceste probleme sunt tolerate în folosința sistemelor.

Timpi de răspuns și rezoluții

Timpii de răspuns și rezoluțiile problemelor sunt stabilite pentru fiecare categorie în parte. La sfârșitul fiecărui caz deschis Furnizorul va efectua o analiză a cauzelor care au dus la producerea deranjamentului și va fi inclusă în recomandarea finală.

Furnizorul va respecta următorii timpi de răspuns:

Timpi de răspuns	Temp soluție provizorie	Temp de remediere
8 ore	A doua zi lucrătoare	best-effort

Timpii de mai sus sunt calculați din momentul în care Furnizorul a fost înștiințat de apariția problemelor.

Furnizorul va garanta că SLA-ul mai sus menționat se bazează pe servicii de suport software furnizate în cadrul acestui contract. În cazul în care apare un deranjament hardware, timpii de răspuns vor fi calculați, deasemenea, pe baza tabelului de mai sus.

Definiții:

Temp de Remediere	Durata de timp până la oferirea soluției finale
Temp de Răspuns	Tempul scurs de la contactul inițial dintre Beneficiar și HELPDESK și răspunsul primit de la echipa de suport tehnic a Furnizorului către Beneficiar. Această acțiune se va desfășura prin intermediul telefonului.
SLA	Service Level Agreement identifică funcționalitățile și definește procesele care implică livrarea de către Furnizor a diferite servicii de suport către Beneficiar.
Subscripție Software	Acces înregistrat la modificări, corectări, și/sau update-uri de Software; incluzând Hotfixuri, Service Packuri, Feature Packs, și/sau upgrade-uri majore, oferite către Beneficiar prin intermediul suportului electronic (e-mail) sau prin suport fix media.
Suport	Telefonul de suport tehnic, asistentă web și e-mail oferite de Furnizor pentru a ajuta Beneficiarul în rezolvarea problemelor apărute. Suportul este oferit la un Major Release al produsului și la un Release Secvențial Anterior al produsului. Furnizorul va oferi de asemenea asistentă tehnică pentru versiunile mai vechi ale produsului, dar rezolvarea problemei ar putea fi limitată la instalarea unui Major Release. Suportul nu include nici un fel de servicii educaționale sau profesionale. Serviciile de training sau de suport on site pot fi achiziționate în plus față de

	cele de Suport.
HELPDESK	Un centru de asistență tehnică ce oferă serviciul de preluare a cererilor prin telefon, web și e-mail operat de către personalul care face parte din suportul Furnizorului oferind asistență cu diagnosticare și rezoluție a defecțiunilor și/sau avariilor apărute în cazul produselor CheckPoint care sunt în conformitate cu documentația publicată când produsele sunt instalate și utilizate conform specificațiilor software-ului CheckPoint.
Remediere Temporară	O modificare în cadrul procedurilor sau datelor care să evite erorile fără folosirea defectuoasă a produselor.

Mentenanța licențelor achiziționate

Servicii Suport Furnizor

Furnizorul va furniza Servicii de Mentenanță după lansarea în producție a sistemului, care vor cuprinde:

- Suport pentru customizările și dezvoltările / extensiile din cadrul implementării
- Suport pentru produsele/modulele utilizate în dezvoltarea sistemului informatic
- Suport pentru platforma hardware/ sistem de operare utilizată

Pentru a permite o identificare proactivă a unor posibile soluții, se va asigura acces la o bază de cunoștințe tehnice și/sau documentație tehnică specifică.

Suport implementare:

Echipa de implementare va asigura suport la darea în producție pe o perioadă de 60 de zile. După această perioadă va fi desemnat un singur punct de intrare pentru toate incidentele legate de soluția implementată și anume către Administratorul de Servicii al Furnizorului. Administratorul de Servicii al Furnizorului va:

- administra și monitoriza incidentele,
- lua legătura cu persoana desemnată ca punct de contact din partea Beneficiarului, pentru analiza stărilor incidentelor deschise,
- va răspunde tuturor întrebărilor legate de incidente.

Suportul va fi furnizat între [09:00 și 18:00] ora României, de Luni până Vineri cu excepția sărbătorilor legale.

Se va asigura diagnosticarea unui incident pentru determinarea problemei de bază. Se va monitoriza în permanență incidentul până la închiderea acestuia.

Urmărirea incidentelor

Persoana desemnată ca punct de contact din partea Beneficiarului va lansa un incident, Administratorul de Servicii al Furnizorului primind o notificare pe e-mail sau fax. Fiecare incident va avea atașat un nivel de prioritate (ca în exemplele de mai jos) care să reflecte impactul problemei asupra funcționării sistemului. Inițial atașarea nivelului de prioritate se va face cu ajutorul Administratorului de Servicii al Furnizorului pentru a facilita rezolvarea incidentului în timp util. Nivelul de prioritate poate fi modificat cu acordul părților în funcție de evoluția incidentului. Furnizorul poate să își rezerve dreptul de a modifica un incident dar cu anunțarea în avans a echipei Beneficiarului

Serviciile de Suport vor fi furnizate sub incidenta Clauzelor de Confidențialitate.

Asistenta poate fi de două tipuri:

- on site (la sediul clientului acolo unde e posibil)
- remote (clientul este responsabil să asigure acces VPN consultaților care vor remedia problema)

Nivele de Prioritate:

Nivel Prioritate	Descriere
Urgent	<p>Impact Major asupra funcționării sistemului</p> <p>Problema împiedică desfășurarea activității instituției, procesul de activitate este serios afectat și nu mai poate continua pierderea funcționalităților devenind critice.</p> <p>Un incident de Nivel 1 are una sau mai multe din următoarele caracteristici:</p> <ul style="list-style-type: none">• Date corupte• Funcții importante indisponibile• Sistemul este “agățat” cauzând întârzieri neacceptabile în accesul la resursele sistemului și/sau în timpul de răspuns• Căderea completă a sistemului sau căderi repetate după restart

Critic	Impact Semnificativ asupra funcționării sistemului Problema împiedică desfășurarea în condiții normale a activității utilizatorilor. Nici o soluție alternativă nu este disponibilă, iar activitatea utilizatorilor poate totuși continua, însă într-un mod restrictiv.
Major	Impact Mediu asupra funcționării sistemului Problema afectează minor funcționalitățile sistemului. Impactul reprezintă un inconvenient care necesită soluții alternative pentru refacerea funcționalităților.
Minor	Impact Minim asupra funcționării sistemului Problema nu afectează funcționalitățile sistemului. Rezultatul este o eroare minoră care nu împiedică desfășurarea în bune condiții a activității utilizatorilor.

În cazul incidentelor cu nivel de prioritate "urgent" asistența va fi asigurată 24x7, fiind disponibilă până când problema va fi rezolvată. Pentru aceasta Beneficiarul va furniza o persoană de contact, disponibilă 24x7, care să furnizeze informații, să testeze soluții și să aplice soluțiile furnizate.

Furnizorul va furniza următoarele Servicii de Mentenanță pentru Extensii (customizări și dezvoltări):

- Furnizorul va asigura suport pentru extensii dacă problema este de tip funcțional sau de performanță ce derivă din funcționalitățile din documentațiile referitoare la eventualele extensii.
- Serviciile post-implementare vor fi oferite către Beneficiar în cadrul unui contract separat pentru toate customizările și modificările efectuate pe perioada desfășurării proiectului, în concordantă cu activitățile descrise mai sus.

7.2 Sustenabilitate

Sustenabilitatea instituțională va fi realizată prin:

- instruirea a minim 10 utilizatori ai soluției care urmează a fi achiziționată
- instruirea a minim 4 persoane care vor asigura administrarea soluției.

După implementare, Beneficiarul va asigura atât operarea noului sistem cât și suport tehnic, după cum urmează:

Operare:

- Autentificare / Autorizare;
- Informare;
- Acces la proceduri electronice;
- Tracking & History;

Suport:

- Probleme tehnice ale soluției;
- Aspecte legate de utilizarea portalului, crearea fluxurilor de documente, etc.;

Beneficiarul va defini grupuri care vor fi implicate în implementarea proiectului și care vor asigura ulterior menținerea rezultatelor după cum urmează:

- Un grup cu atribuții de susținere a implementării soluției informatice având ca responsabilitate următoarele atribuțiuni de bază:
 - implementarea aplicațiilor pentru domeniile de activitate ale instituției;
 - informatizarea activităților;
 - elaborarea și validarea specificațiilor tehnice;
- Un grup responsabil atribuții de analiză funcțională responsabil cu:
 - analiza proceselor care vor fi derulate în urma implementării soluției informatice;
 - elaborarea și validarea specificațiilor funcționale.