# Ministerul Afacerilor Externe din România

## Centru unic de contact şi suport

## CUPRINS

# 1.Introducere, informații generale

Strategia națională privind relațiile cu românii de pretutindeni are la bază principiul identificării soluțiilor adecvate situațiilor particulare existente în cadrul comunităților românești din spatiul UE și nu numai.

Se urmarește în mod permenent păstrarea și întărirea legăturilor dintre România și comunitățile românești din emigrație. conform standardelor internaționale în materie.

În momentul de față se estimează peste 3 milioane cetățeni români în emigrație aflați în spațiul UE și aproximativ 2 milioane în spatiul non UE. Pentru aceste categorii de cetățeni, MAE, prin consulatele și ambasadele sale, oferă următoarele tipuri de servicii:

- documente de călătorie: pașaportul simplu electronic; pașaportul simplu temporar; titlul de călătorie; pașaportul simplu pentru cetățenii români cu domiciliul în străinătate;
- acte de stare civilă: înscrierea certificatelor de stare civila emise de autorități străine; obținerea actelor de stare civilă din România;
- certificate de cazier judiciar;
- acte notariale: autentificarea procurilor și declarațiilor; legalizarea copiilor de pe înscrisuri; legalizarea traducerilor; legalizarea semnăturilor;
- cetațenia română redobândirea cetățeniei române: (redobandirea cetățeniei române pierdută după 22 decembrie 1989; redobandirea cetățeniei române pierdută înainte de 22 decembrie 1989); renunțarea la cetățenia română; clarificarea cetățeniei române;
- prelucrarea datelor personale.

În furnizarea acestor servicii s-au constatat următoarele neajunsuri :

- necunoașterea de catre cetățenii români a drepturilor și obligațiilor în țările UE și non UE în care călătoresc;
- necunoașterea de către cetățenii români a regimului contractelor de muncă din țara respectivă
- acuzația de "indiferență" adusa statului roman fata de etnicii romani care solicita redobandirea cetateniei romane, datorita perioadei nedefinite de rezolvare a redobandirii cetateniei romane (problema oarecum rezolvata prin infiintarea Agentiei Nationale de Cetatenie)
- lipsa inregistrarii cetatenilor romani la sediile oficiilor diplomatice si consulare din zona de resedinta
- insuficienta personalului consular
- practica generata de fenomenul "Polonia" cand un cetatean roman a murit in greva foamei
- vizitele la penitenciare, reduse in contextul in care unele misiuni functioneaza cu un singur reprezentant consular
- durata mare de raspuns a autoritatilor locale in rezolvarea unor probleme legate de retrocedarea proprietatilor cetatenilor romani
- clarificarea cetățeniei române datorită prezenței unui număr mare de falsuri în acte, identificate pe parcursul verificărilor.

Proiectul propus constă în inființarea unui centru unic de contact si suport pentru cetatenii romani din strainatate care sa intareasca si sa diversifice actualele servicii specifice ale consulatelor si ambasadelor MAE, sporind astfel imaginea MAE in străinătate.

# 2.Obiectivele Proiectului

Scopul principal al proiectului este înființarea unui centru unic de contact și suport pentru cetățenii români din străinătate care să întărească și să diversifice actualele servicii specifice ale consulatelor și ambasadelor MAE, sporind astfel imaginea MAE în străinătate.

## 1.Obiective generale

Proiectul se înscrie și în direcția prioritară de acțiune a diplomației române în 2013 și anume Acordarea atenției cuvenite românilor din străinătate. Prin intermediul centrului unic de contact și suport MAE va avea un instrument eficient de comunicare cu cetățenii, fiind mai aproape de problemele sesizate de către aceștia, precum și un instrument de monitorizare și urmărire a modului cum aceste sesizări au fost soluționate de către personalul MAE.

În pofida constrângerilor financiare, MAE va continua eforturile menite să ofere cetățenilor români sau etnicilor români care trăiesc/muncesc în străinătate sprijin, asistență și servicii de proximitate de o manieră compatibilă cu statutul nostru de țară membră UE și cu normele în domeniu. MAE va acorda o atenție sporită asigurării unei asistențe adecvate și eficiente pentru cetățenii români aflați în zonele de conflict.

Modul în care sunt respectate identitatea, drepturile și valorile spirituale ale comunităților românești din alte țări, inclusiv cele învecinate, reprezintă o preocupare majoră pentru MAE și va constitui în continuare un criteriu important de evaluare a relațiilor bilaterale.

Progresele înregistrate până în prezent vor fi consolidate. În mod concret, MAE își propune în 2013 deschiderea unor consulate românești noi, implementarea unor proiecte în vederea facilitării accesului la serviciile consulare (acte de stare civilă, documente de călătorie, vize, acte notariale, taxe consulare), precum și continuarea modernizării rețelei consulare a României.

Aderarea la spațiul Schengen rămâne un obiectiv strategic pentru România. Demersurile prioritare vor viza prezentarea argumentelor în favoarea unei decizii pozitive în cursul acestui an – pornind de la realitatea îndeplinirii de către partea română a condițiilor obiective de aderare –, astfel încât să poată fi depăşit blocajul actual generat de o poziție singularizată printre țările membre.

În cadrul Mecanismului de Cooperare şi Verificare, MAE, alături de celelalte ministere implicate, va continua să prezinte cu acuratețe, pe baza progreselor interne realizate, îndeplinirea angajamentelor asumate, circumscrise obiectivului de consolidare a unui sistem judiciar corect şi eficient, orientat către cetățean. MAE va contribui la identificarea şi promovarea formulei cele mai favorabile intereselor României, în contextul evaluării Comisiei Europene din vara 2012 privind cei 5 ani de la crearea mecanismului şi posibila lui încetare/transformare.

MAE va urmări reflectarea eforturilor României privind integrarea romilor şi va facilita dialogul partenerilor europeni cu instituțiile competente din România privind Strategia națională de incluziune a romilor 2012-2020, adoptată în decembrie 2011, sprijinind obținerea de progrese vizibile în aplicarea acesteia.

## 2.Obiective specifice

Proiectul se încadrează în obiectivele şi operaţiunile domeniului major de intervenție 2.*2* ***Îmbunătățirea calității şi eficienței furnizării serviciilor*** prin:

- îmbunătățirea calității serviciilor publice oferite de serviciile consulare ale MAE
- consolidarea capacității administrative de gestionare a proceselor complexe de furnizare a serviciilor către cetățeni, în special ceea ce priveşte asigurarea calității şi a promptitudinii în soluționarea cererilor cetățenilor.

Obiectivele specifice ale proiectului sunt:

- Ameliorarea sensibila a problematicii legata de necunoaşterea de către cetățenii romani a drepturilor și obligațiilor pe care le au într-o țară străină
- Creşterea gradului de satisfacție în rândul publicului prin oferirea posibilității de a accesa informații cu caracter consular în timp util,
- Eficientizarea muncii angajaților serviciilor consulare române, prin faptul că o parte din problemele semnalate se pot rezolva fără implicarea lor directă susținând astfel prioritățile MAE pe termen mediu;
- Contribuția serviciului consular la conturarea profilului României de membru responsabil, eficient, pragmatic şi influent al UE, la îndeplinirea angajamentelor asumate în perioada de preaderare şi la asigurarea predictibilității acțiunii la nivel comunitar şi a condițiilor pentru o prestație la nivelul aşteptărilor pe care le au factorii de decizie şi cetățenii din România, dar şi partenerii din Uniune.
- Îmbunătățirea serviciilor consulare adresate cetățenilor români aflați în străinatate;
- Continuarea reformei instituționale şi următoarele direcții de activitate din Planul Strategic de Dezvoltare a MAE
- Urmărirea intereselor internaționale şi interne ale României în plan multilateral şi prin proiecte speciale de politică externă
- Promovarea şi sprijinirea intereselor cetățenilor români şi realizarea activităților consulare prin:
    - creșterea vitezei de răspuns la solicitarile primite de la cetățeni,
    - prioritizarea problemelor semnalate
    - oferirea de servicii diferențiate pe zone geografice, în funcție de meridian, limbă sau comunitate, să cuantifice problematica întampinata şi soluțiile oferite şi să îmbunătățească procedurile, să reducă timpul de răspuns.
    - pune la dispoziția cetățenilor a unui punct de acces unitar apelabil prin numere de telefon locale (în fiecare țară, regiune, în funcție de personalul consular responsabil alocat) sau internațional disponibile 24 de ore pe zi, 7 zile pe saptamână.
    - punerea la dispozitia personalului diplomatic și consular a unor instrumente de preluare, analiza și soluționare a problematicilor relevante care țin de competența acestora
    - obtinerea, la nivelul MAE de rapoarte centralizate și statistici cu privire la problematicile întâmpinate de către cetățenii români aflați în străinatate
    - realizarea unei baze de date centralizate cu soluțiile propuse de personalul consular pe diferite problematici si descrierea practicilor de succes cu referire la acestea

# 3.Descrierea soluției

Pentru acoperirea obiectivelor specifice ale proiectului, MAE dorește implementarea unei Sistem Informatic Integrat de tip Contact Center.

Acesta va permite integrarea următoarelor servicii într-un unic punct de contact:

- preluarea intr-un mod unitar a cererilor cetățenilor referitoare la cazuistica specifică pe diverse canale de comunicare: telefon, web, mail, instant messaging. Acolo unde este posibil, cetățenii vor putea incarca în sistem copii scanate ale documentelor necesare soluționării cererilor acestora
- clasificarea și tratarea cazurilor preluate pe diversele canale de comunicare
- introducerea de fluxuri automate de tratare a solicitărilor si problemelor semnalate funcție de categoria în care se încadrează
- oferirea de informații specifice în cadrul site-ului centrului de contact
- transmiterea de mesaje automate de răspuns la cazurile semnalate (pe email, telefon) către cetățeni, acolo unde este posibil

Sistemul informatic integrat va fi implementat folosindu-se o infrastructură hardware și software care să asigure securitatea acestuia la nivel de rețea, de aplicații, de date si de utilizator prin integrarea de echipamente hardware și de soluții software specifice

Sistemul va permite următoarele acțiuni:

- Preluare apeluri de la cetățenii români aflați în străinatate şi înregistrare solicitări/probleme în sistemul informatic;
- Oferirea de consultanță consulară imediată pentru problemele semnalate sau de informații cu caracter consular;
- Oferirea de consultanță juridică imediată pentru solicitările de acest gen;
- Direcționarea cetaţenilor conform normelor şi regulilor MAE către organisme locale/naționale în vederea soluționarii problemelor/solicitărilor semnalate;
- Semnalarea cazurilor deosebite direct organelor abilitate naționale (MAE, MAI) sau celor locale de urgență (poliție, ambulanță, pompieri etc);
- Stocarea şi centralizarea informațiilor despre cazuri, soluții, cu respectarea legislatiei in vigoare privind protectia datelor cu caracter personal;
- Auditarea activităților angajaților MAE (atât a agenților din Call Center cât şi a personalului consular -care opereaza in cadrul sistemului);
- Eficientizarea comunicării între MAE şi cetățean, precum şi asigurarea transparenței activității prin publicarea de rapoarte de activitate;
- Monitorizarea şi evaluarea modului de soluționare a problemelor/solicitărilor semnalate;
- Generarea de rapoarte în funcție de perioadă, zonă geografică, tipologii de probleme/solicitări, respectiv soluții şi a timpului de răspuns.

Oferirea de servicii diferențiate pe zone geografice, în funcție de meridian, limbă sau comunități se referă la:

- Regimul de vize
- Acte normative
- Asistența consulară

- Ce pot face funcționarii consulari pentru dvs.
- Ce nu pot face funcționarii consulari
- Unde puteți cere asistență consulară
- Despre consulii onorifici
- Accidente
- Imbolnăviri
- Decese
- Acte furate sau pierdute
- Arestare
- Prelucrarea datelor personale
- Riscuri de securitate cauzate de acțiuni teroriste
- Asistență consulară europeană
- Documente de călatorie
- Paşaportul simplu electronic
- Paşaportul simplu temporar
- Paşaportul simplu pentru cetaţeni români cu domiciliul în strainătate
- Titlul de călătorie
- Acte notariale
- Aplicarea apostilei în România
- Acte de stare civilă
- Serviciul de stare civilă S1
- Înscrierea documentelor emise de autoritățile străine
- Obținerea documentelor din România
- Căsătoria în străinătate
- Cetăţenia română
- Clarificarea cetățeniei române
- Redobândirea cetățeniei române
- Renunțarea la cetățenia română
- Legalizări documente
- Procedura de supralegalizare
- Formulare consulare
- Taxe consulare

Prin faptul că pune la dispoziția cetățenilor un serviciu de tip “Call Center” prin intermediul telefonului/ internetului, care va asista în procesul de soluționare a cazurilor semnalate de cetățenii români aflați în străinătate, proiectul va contribui la creşterea gradului de satisfacție în rândul publicului prin oferirea posibilității de a accesa informații cu caracter consular în timp util.

Proiectul are în vedere, de asemenea, şi eficientizarea muncii angajaților serviciilor consulare române, prin faptul că o parte din problemele semnalate se pot rezolva fără implicarea lor directă susținând astfel prioritățile MAE pe termen mediu:

- Contribuția serviciului consular la conturarea profilului României de membru responsabil, eficient, pragmatic şi influent al UE, la îndeplinirea angajamentelor asumate în perioada de preaderare şi la asigurarea predictibilității acțiunii la nivel comunitar şi a condițiilor pentru o prestație la nivelul aşteptărilor pe care le au factorii de decizie şi cetățenii din România, dar şi partenerii din Uniune.
- Introducerea sistemului va conduce la posibilitatea procesării unui numar estimat de 2

milioane de cereri de servicii consulare pe an
- Îmbunătățirea serviciilor consulare adresate cetățenilor români aflați în străinatate;
- Continuarea reformei instituționale şi următoarele direcții de activitate din Planul Strategic de Dezvoltare a MAE
- Urmărirea intereselor internaționale şi interne ale României în plan multilateral şi prin proiecte speciale de politică externă
- Promovarea şi sprijinirea intereselor cetățenilor români şi realizarea activităților consulare

# 4.Beneficiarii proiectului

Grupul țintă (beneficiarii direcți ai proiectului) este reprezentat de 500 de persoane, personal din cadrul MAE care vor utiliza sistemul şi vor deveni mai competitivi şi eficienți în realizarea sarcinilor de serviciu. 100 de persoane vor fi selectate din cadrul MAE – Direcția Generală Afaceri Consulae şi 400 de persoane vor fi selectate din cadrul Misiunilor Diplomatice ale României (135 de consuli şi 265 de funcționari consulari).

Beneficiari indirecți sunt reprezentați de:

- 4 milioane cetățeni români în emigrație aflați în spațiul UE
- 2 milioane cetățeni români aflați în spațiul non UE, care solicită în mod frecvent asistență din partea instituțiilor consulare.

După ultimele evidențe de la Direcția Consulară din cadrul MAE, se înregistrează anual peste 1.000.000 cereri/solicitări pe diverse cazuri (pierderi/furt acte, solicitări de prelungire acte, asistență juridică, repatrieri, legalizări etc), astfel că se estimează ca prin intermediul realizării acestui proiect numărul de solicitări se va dubla, ceea ce se transpune în aproximativ peste 2.000.000 solicitări, deci beneficiari pe an (dintre cetățeni).

- Pentru o mai bună înțelegere a componentei grupului țintă precizăm că din grupul de 500 de persoane vor face parte:MAE, Direcția Generală Consulară – 100 de persoane
- Personal din Misiunile diplomatice – 135 de consuli şi 265 de funcționari consulari.

În acest moment în cadrul MAE - Direcția Generală Consulară sunt angajate 100 de persoane, iar ca personal care functionează în cadrul misiunilor diplomatice sunt 400 de persoane în 135 de locații, care oferă suport şi informații în următoarele domenii:

- documente de călătorie: paşaportul simplu electronic; paşaportul simplu temporar; titlul de călătorie; paşaportul simplu pentru cetățenii români cu domiciliul în străinătate.
- acte de stare civilă: înscrierea certificatelor de stare civilă emise de autorități străine; obținerea actelor de stare civilă din România.
- certificate de cazier judiciar.
- acte notariale: autentificarea procurilor şi declarațiilor; legalizarea copiilor de pe înscrisuri; legalizarea traducerilor; legalizarea semnăturilor.
- cetățenia romană: redobândirea cetățeniei române: (redobândirea cetățeniei române pierdută după 22 decembrie 1989; redobândirea cetățeniei române pierdută înainte de 22 decembrie 1989); renunțarea la cetățenia romană; clarificarea cetățeniei române
- prelucrarea datelor personale.

# 3.Cerințe tehnice și funcționale

Acest capitol descrie principalele aspecte ce vor sta la baza realizării ofertelor tehnice, funcționale și financiare. Cerințele descrise sunt minime și obligatorii, fiecare ofertant trebuind să descrie detaliat si complet într-o matrice de conformitate modul de realizare/satisfacere a fiecărei cerințe sau specificații. Nerespectarea oricărei cerințe din prezentul caiet de sarcini atrage după sine descalificarea ofertei.

Oferta tehnică și funcțională trebuie să fie clar exprimată, să nu dea alternative sau să nu indice drept soluție materiale publicitare (broșuri, site-uri WEB) generale.

Fiecare afirmație din matricea de conformitate trebuie să fie justificata clar și fără a lăsa loc la interpretări și trebuie a fi motivată prin referințe la anexa tehnică ce cuprinde broșuri de produs, referințe WEB sau documentație tehnică– white paper.

NU VOR FI LUATE IN CONSIDERARE MATRICI DE CONFORMITATE COMPLETATE PRIN COPIEREA CERINTELOR IN COLOANA CU PRODUSE OFERTATE, FARA REFERINTE LA ANEXE TEHNICE .

**În cazul în care autoritatea contractantă consideră că informațiile cuprinse in ofertele tehnice ale ofertanților nu sunt concludente la nivel de descriere, aceasta poate solicita sesiuni demonstrative în vederea validării acoperirii funcționalităților solicitate din prezentul caiet de sarcini.**

## 1.Locul de implementare a proiectului

Centrul de contact şi suport pentru cetățenii români din străinătate se va implementa la nivelul sediului central al Ministerului Afacerilor Externe – Aleea Alexandru nr. 31, Sector 1, Bucureşti, cu sprijinul Direcției Schengen – str. Ermil Pangratti nr. 20, Sector 1, Bucureşti. În cadrul MAE se va înființa centrul de contact şi suport unde agenții (angajați ai ministerului) vor răspunde la apelurile cetățenilor 24 de ore, 7 zile pe săptămână.

La nivelul fiecărei reprezentanțe diplomatice se va livra infrastructura necesară interconectării cu centrul de contact şi se va asigura punerea în funcțiune a soluției.

Lista reprezentanțelor diplomatice ale MAE este prezentată in ***Anexa 1 – Lista locațiilor proiectului***.

## 2.Arhitectura funcțională

Componentele principale ale solutiei care vor fi implementate sunt:

A. Zona de servicii tip « PORTAL » - are urmatoarele caracteristici:

- ofera servicii de informare si consultanta diferentiate pe zone geografice, in functie de meridian, limba sau comunitati, pe baza selecțiilor realizate de utilizator/petent ;
- implementează noi canale de comunicare (e-mail si alte tipuri de mesaje in format

electronic) ;

- oferă asistență specializată din partea unui personal dedicat pe toate aceste canale de comunicație ;
- oferă servicii specifice si de interes comunităților – domenii de muncă, evenimente/divertisment, propuneri de colaborare, schimburi de informație/experiență, etc ;
- oferă servicii de preluare/emitere de diverse documente de interes pentru cetățeni ;

B. Zona de servicii tip « CALL CENTER » - are următoarele caracteristici:

- oferă servicii de informare și asistență telefonică specializate pe comunități și limbă ;
- implementează noi canale de comunicare (fax) ;
- oferă asistență specializată din partea unui personal dedicat pe acest(e) canal(e) de comunicație
- oferă servicii de gestiune a relației cu cetățenii (componenta pseudo-CRM) ;

C. Zona de servicii de « ANALIZĂ » - are următoarele caracteristici:

- Va permite constituirea unei baze de date (tip Data Warehouse) care să stocheze informații de interes privind cetățenii români din afara țării. Aceasta bază va fi necesară pe de o parte pentru MAE pentru a-și face o imagine corectă asupra numărului de cetățeni români aflați în emigrație, asupra nivelului de pregătire/zonele de emigrație, folosind diversi indicatori statistici și sociologici privind cetățenii români din străinătate, iar pe de alta parte chiar cetățenilor, pentru a fi îndrumați mai eficient în căutările lor în cadrul portalului ;
- Implementează o componentă specifică de Business Intelligence, care sa ofere MAE o structură solidă de raportare pe diverși indicatori pentru uz intern și către alte instituții interesate;

Functionalitățile celor 3 zone vor fi implementate prin intermediul următoarelor subcomponente:

- Centrul de preluare a apelurilor dotat cu IVR (CallCenter)
- Platforma portal
- Componenta front-end web de balansare a încărcării
- Sistem de gestiune a tichetelor(Componenta colaborativa tip CRM)
- Componenta de analiză și raportare
- Componenta de gestiune a identitatii utilizatorilor MAE
- Subcomponenta de securitate a sistemului informatic
- Aplicația Antivirus
- Baza de date de tip enterprise
- Subcomponenta de administrare a sistemului informatic
- Software de educare și pregătire a operatorilor (e-Learning)
- Aplicația pentru securizarea Call Center MAE
- Software  virtualizare și management servere
- Platforma de virtualizare tip desktop
- Software mesagerie electronică

Schema bloc funcțională a sistemului integrat este prezentată  în figura de mai jos:

Soluția ofertată trebuie să fie în concordanță cu schema bloc prezentată mai sus. În cadrul soluției ofertate se va explicita în mod detaliat din punct de vedere tehnic și funcțional fiecare componentată a schemei bloc prezentate. Toate subcomponentele din lista de mai sus trebuie sa aibă la bază produse software de tip COTS (Commercial of the shelf).

Soluția ofertată va fi complet funcțională și va include toate licențele necesare, autoritatea contractantă nu pune la dispozitie licențe sau echipamente suplimentare.

# 3.Arhitectura tehnică

În figura de mai jos este prezentată arhitectura tehnică ce trebuie să deservească Centrul de Contact al MAE. Figura este o prezentare generală, astfel încât ofertanții să respecte principiile generale ale prezentului caiet de sarcini permitând să construiascăși să prezinte soluții conforme cu cererea.

Fiecare ofertant trebuie să prezinte o schema detaliată a componentelor arhitecturii, astfel încât să rezulte clar și neinterpretabil, următoarele:

- Interconectarea logică și funcțională a componentelor sistemului; diagrame de flux de informații; diagrame de flux de date;
- Sistemele hardware componente ale arhitecturii cu nume, configurație și componența principală (ex pentru servere : Procesoare – tip și frecvență, memorie, numarul și tipul sloturilor I/O, Sistem de operare);
- Arhitectura conexiunilor LAN, WAN, FC și alimentare;
- Sistemele de operare ce rulează pe fiecare server;
- Aplicațiile de nivel înalt ce rulează pe fiecare server;
- Schemele de funcționare în caz de defecțiune sau oprire în vederea mentenației a diverselor componente, însoțite de scenarii posibile pentru configurații de siguranță;

Toate echipamentele furnizate în cadrul acestui proiect trebuie să fie noi și să fie acoperite de garanție pentru o perioadă de 5 ani de la data livrării și a acceptanței cantitative si calitative (în cazul unităților de alimentare, garanția trebuie să acopere și bateriile).

Infrastructura HW ofertată trebuie să contina servere dedicate pentru aplicațiile de Call Center telefonie si virtualizare desktop si o solutie de tip blade pentru toate celelalte componente ofertate.

Din motive de ergonomie, securitate, mentenanță și administrare facilă, cele 30 de posturi de operatori trebuie să îndeplinească următoarele caracteristici minime și obligatorii:

- Operatorul trebuie să poată lucra de la oricare din terminale, inclusiv în cursul aceluiași schimb de serviciu
- Fiecare post de lucru trebuie să funcționeze 24 de ore din 24, eventualele opriri fiind doar în cazul înlocuirii de echipamente defecte, sau pentru mentenanță programată.
- Pentru nici unul din posturi nu este permisă salvarea vreunei informații pe suport electronic, magnetic sau optic
- Administrarea mediului de lucru trbuie să se facă centralizat, fără impact în timpul de acces la postul de lucru.

Toate echipamentele centrale trebuie să fie integrate într-un cabinet standard IT de 42 U prevăzut cu uși

față/spate, ambele prevăzute cu cheie. Cabinetul trebuie să fie echipat cu ghiduri de cablu, PDU redundant care să asigure minim 30% spațiu neocupat.

Toate echipamentele din centrul de date, corespunzătoare proiectului trebuie sa fie alimentate redundant, UPS-ul asigurând o funcționare de minim 15 minute după interuperea alimentării.

Componentele critice ale arhitecturii fizice și logice trebuie să fie asigurate împotriva căderilor/defecțiunilor accidentale prin mecanisme de redundanță. Elementele critice ale arhitecturii sunt:

- Platforma portal
- Serverul pentru baze de date care stochează informațiile din aplicații
- Sistemul de gestiune a tichetelor
- Centrul de preluare a apelurilor dotat cu IVR
- Echipamentul de stocare de date și SAN
- Infrastructura ce asigură securitatea sistemului
- Infrastructura ce asigură accesul utilizatorilor la sistem

Întreaga arhitectură (excepțiile fiind menționate explicit) trebuie să fie instalată într-un mediu virtualizat, licențiat corespunzător. Fiecare ofertant va justifica în detaliu, indicând surse autorizate (site-uri ale producătorilor, scrisori de sustinere a producătorilor) că licențierea este acoperitoare pentru soluția ofertată. Oferta tehnică trebuie să indice în mod clar în ce mod soluția de virtualizare nu scade performanța aplicațiilor fata de absenta acesteia, inclusiv în cazul unei situații de minimă acoperire a funcțiilor.

Toate elementele critice ale arhitecturii soluției trebuie să fie asigurate în configurații de înaltă disponibilitate, fără puncte singulare de cădere sau în configurații care să permită distribuirea încărcării între nodurile aceluiași subsistem.

Soluția trebuie să dispună de o inferfată unică de management al utilizatorilor privilegiați atât la nivelul sistemelor de operare virtualizate cât și la nivelul platformei de virtualizare propuse.

# 4. Cerinte generale ale sistemului informatic Centru de Contact şi Suport pentru Cetățenii aflați în Străinătate

## 1. Cerințe generale de business

În imaginea de mai jos este prezentată schema generală a unui flux de lucru ce trebuie implementat în cadrul proiectului.

Proiectul Centru de Contact şi Suport pentru Cetățenii Români aflați în străinătate doreşte îmbunătățirea serviciilor MAE acordate cetățenilor aflați în dificultate.

Prin sistemul de Call Center cetățeanul apelează un număr de telefon local pus la dispoziție de către Ministerul Afacerilor Externe în fiecare țară unde are reprezentanță diplomatica. Apelul va fi transferat prin centrala telefonică a consulatului în rețeaua de telefonie MAE şi transmis în sistemul de preluare a apelurilor dotat cu IVR. Prin meniul IVR prestabilit numeric de la 1 la 9 se vor soluționa apeluri de tip informativ, unul dintre meniuri va fi pentru a intra în legătura cu unul dintre operatori (agenți) din centrul de suport. Operatorul va prelua cazul prin intermediul portalului, în aplicația de

gestiune a apelurilor va deschide un bon (tichet) şi va încerca să răspundă apelantului. Dacă operatorul îi oferă informația necesară apelantului bonul va fi închis pe baza de cunoştințe din call centre. Dacă informația sau situația depăşeşte competențele operatorului, cazul este transferat către supervizor. În situația cazurilor excepționale (situații grave, conflictuale), supervizorii pot înainta solicitarea pe fluxul intern, conform procedurilor specifice MAE, în vederea soluționării. După soluționarea cazului, tichetul va fi închis, ataşând la acesta informațiile sau documentele necesare de pe flux. Sistemul va păstra istoricul tichetelor/cazurilor semnalate şi rezolvate în acest mod.

Prin sistemul de portal, cetățenii care au acces la internet vor putea accesa un portal al cărui nume va fi definit, care va oferi o bază de cunoştințe sau o listă de întrebări frecvente unde vor fi postate informații generale, ghiduri şi recomandări pentru soluționarea unor situații uzuale de tip: contact cel mai apropiat consulat, demersuri in caz de pierdere documente, cereri audiență, solicitare documente consulare etc. Pentru situațiile care nu se regăsesc în baza de cunoştințe, portalul va oferi posibilitatea de a deschide un bon (tichet) on-line, printr-un formular special. Acest tichet va fi preluat de unul dintre operatorii din call centre, care va urmări fluxurile de soluționare a cazurilor semnalate conform procedurilor MAE. Cetățeanul care a deschis tichetul on-line va fi contactat de către operator, pe baza datelor de contact din tichet (telefon, e-mail), va fi informat cu privire la soluționarea cazului, apoi tichetul este închis şi se arhivează în baza de cunoştințe.

Platforma portal va avea rol de publicare informații interne, dashboarduri, statistici cu privire la cazuri si soluționarea acestora. Sistemul informatic va încorpora aplicațiile:

- Aplicația pentru gestiunea cazurilor tip CRM
- Aplicația pentru managementul bazelor de date
- Managementul infrastructurii și a aplicațiilor
- Platforma de educare și pregătire a operatorilor
- Componenta de front-end web.

Platforma portal se va integra cu sistemul de mesagerie electronică ofertat. Celelalte componente vor fi suport pentru funcționarea aplicațiilor enumerate în fluxul operațional.

## 2. Cerințe generale funcționale

- Sistemul va dispune de o funcționalitate de gestiune a conținutului de date stocate în vederea expunerii acesteia în zona publică a portalului
- Sistemul va permite integrarea cu alte sisteme prin servicii web care pot fi folosite de aplicațiile externe pentru a introduce date în sistem prin transmiterea de XML-uri, în conformtate cu modelele informaționale de introducere de date
- Sistemul va permite folosirea de plug-in-uri care pot fi create pentru comunicație și schimb de date cu sisteme de terță parte și pot fi administrate independent.
- Sistemul va permite urmărirea evoluției fluxurilor și realizarea de rapoarte, precum și transmiterea de notificări către utilizatorii implicați;
- Sistemul informatic va dispune de o componentă de analiza incluzând atât funcționalități clasice de raportare cât și functionalități de analiză multidimensională și vizuală,
- Toate configurările sistemului trebuie executate utilizând exclusiv instrumentele vizuale ale interfețelor componentelor ce compun sistemul integrat.

## 3. Cerințe generale de securitate

- În afara zonei sale publice, sistemul va permite accesul auditat și restricționat în funcție de

drepturile fiecărui grup de utilizatori în parte, administrate cu ajutorul rolurilor și al listelor de permisiuni.
- Sistemul va permite gestionarea de conturi de utilizator, grupuri, roluri, permisiuni și drepturi de acces prin intermediul unei interfețe generice
- Sistemul va conține un conector de integrare cu structura de Active Directory existenta, aceasta oferind posibilitatea de autentificare automată în sistem, în baza contului de domeniu.
- Autentificarea utilizatorilor în sistem, pentru zonele care nu sunt publice, se va efectua pe baza de utilizator si parolă dar și pe baza de certificat digital stocat pe dispozitivul criptografic tip token USB
- Sistemul va folosi un mecanism general de evidență și constituire a logurilor pentru cele mai importante acțiuni efectuate în cadrul acestuia

În vederea asigurării unui nivel ridicat de protecție a datelor, platforma va trebui să respecte următoarele cerințe:

- Să asigure criptarea datelor care sunt stocate în baza de date, la nivel de coloană, tabelă sau tablespace.
- Să asigure criptarea traficului prin rețea între utilizator, aplicație şi baza de date, pentru a elimina posibilele încercări de interceptare a datelor când sunt transmise în mediile de comunicație.
- Să asigure confidențialitatea informațiilor vehiculate în conformitate cu modul de exploatare, pe verticală şi pe orizontală, a resurselor informaționale ale sistemului.
- Să blocheze încercarea de utilizare neautorizata de resurse, servicii sau informatii, să inregistreze evenimentul intr-un fisier sau tabela de supraveghere şi să semnaleze în timp real aceste evenimente personalului administrativ.
- Să ofere functionalități de tip single sign-on (autentificare unică) pentru toate resursele protejate; orice utilizator care se autentifică și este autorizat trebuie să poată avea acces la informațiile expuse de sistem, fără a i se cere reautentificarea pe parcursul sesiunii, atât timp cât nu există politici care să ceara acest fapt.
- Să ofere autentificare multi-nivel combinând orice metode de autentificare disponibile (de exemplu nume utilizator și parolă pentru nivel privat, certificat digital pentru nivel confidențial, etc).
- Să suporte cel putin următoarele metode de autentificare:
  - Nume de utilizator si parola;
  - Certificate digitale ITU x.509 v.3;
  - Smart card;
  - Token-uri fizice cu PIN;
  - Bazată pe formulare web;
- Să se integreze cu soluții avansate de raportare și să ofere out-of-the-box rapoarte pentru datele auditate.
- Să realizeze criptarea informației transferata între componentele sistemului și clienți (HTTPS, LDAPS etc).

## 4. Cerințe de scalabilitate și disponibilitate

Pentru a asigura un nivel ridicat de scalabilitate si disponibilitate, platforma trebuie să respecte următoarele cerințe:

- Toate elementele critice ale arhitecturii trebuie să suporte mecanisme de tip clustering

(topologie activ-activ) sau failover (topologie activ-pasiv);

- Să implementeze mecanisme de disponibilitate ridicata (24/7) a aplicatiilor pentru executia continua a serviciilor instalate;
- Să implementeze mecanisme de replicare a obiectelor aplicatiei între serverele aceluiași cluster;
- Să asigure transparența totală pentru utilizatori în momentul apariției unei erori software;
- Să asigure securitate tranzacțională în cazul apariției unor erori hardware sau software în cluster;
- Să asigure protecția bazelor de date împotriva căderilor de tensiune prin realizarea și menținerea de copii multiple ale bazei de producție;
- Să permită atât scalabilitatea pe orizontală, prin adăugarea de noi servere, cât și pe verticală, prin îmbunătățirea capacității serverelor existente.

## 5. Cerințe de fiabilitate și stabilitate

În vederea creșterii fiabilității și stabilității platformei, soluția va trebui să respecte următoarele cerințe:

- Administrarea arhitecturilor de tip cluster;
- Existența unor instrumente pentru realizarea operațiilor de backup si recovery pentru baza de date și pentru aplicații;
- Posibilitatea de a securiza comunicația între diferite componente din platformă.

## 6. Cerințe de extensibilitate

In vederea asigurarii extensibilitatii soluției, platforma va trebui să respecte următoarele cerințe:

- Solutia va avea o arhitectură deschisă, bazată pe standarde deschise: HTML, XML, SOAP;
- Soluția va fi orientată către o arhitectură ce are la bază servicii (Service Oriented Architecture);
- Soluția va oferi integrarea cu sisteme externe existente (LDAP, Server de email);
- Soluția va oferi posibilitatea utilizării serviciilor web pentru a expune date și servicii către sistemele externe aplicației.

## 7. Cerințe generale pentru elementele subcomponente ale arhitecturii soluției

Sistem de Operare pentru echipamentele tip server:

- Să ofere suport pentru instalarea în configurații cluster tip high-availability;
- Să ofere suport pentru tehnologia de virtualizare ofertată;
- Să ofere mecanisme avansate pentru administrare, monitorizare, diagnosticare și recuperare în cazul incidentelor software;
- Să includă mecanisme avansate pentru controlul accesului utilizatorilor la resurse.
- Să fie certificată conform CommonCriteria minim EAL3+

Platforma de virtualizare tip server:

- Să fie compatibilă cu majoritatea producătorilor hardware recunoscuti (ex. IBM, HP, DELL, Fujitsu etc);
- Să ofere suport pentru multiple sisteme de operare;
- Să ofere suport pentru adaugarea de resurse de procesare și memorie fără restartarea sistemului de operare din mașina virtuală;
- Rețeaua virtuală să poată să fie unificată la nivelul întregii infrastructuri virtuale, indiferent de numarul de servere ce fac parte din aceasta infrastructură.

Sistem Antivirus:

- Protectie completa (antivirus, antispyware si antirootkit) pentru sistemul de fisiere;
- Scanare in tip real, optimizata;
- Actualizarea zilnica a bibliotectii de semnaturi de virusi;
- O consola de administrare centralizata pentru toate modulele/componentele solutiei de antivirus.

Platforma de Gestiune a Bazelor de Date:

- Să fie sistem de gestiune a bazelor de date de tip relational;
- Să ofere suport pentru lucrul cu comenzi tip SQL, proceduri stocate, indecsi, triggeri si să permită efectuarea de tranzactii autonome;
- Să ofere suport pentru salvarea/restaurarea precum și arhivarea/dezarhivarea datelor în regim de lucru online;
- Să ofere suport pentru definirea de multiple niveluri de autorizare asupra datelor din baza de date.

Componenta front-end web trebuie să asigure:

- Mecanisme de SSL offloading în cazul securizării comunicației client/server fără a aloca resurse de procesate pentru criptare/decriptare la nivelul server-ului de aplicații
- Reducerea încărcării server-elor de aplicații prin mecanisme de cache-ing al conținutului de tip static
- Reducerea traficului client/server prin mecanisme de compresie a conținutului
- Distribuirea încărcării provenită de la cererile simultane ale clientilor către mai multe server-e de aplicații
- reducerea numarului de IP-uri publice in cazul existentei mai multor server-e de aplicatii.
- Integrarea cu echipamente specifice de accelerare a operatiunilor criptografice cu chei asimetrice (HSM)
- Realizarea unui numar de cel putin 300 de sesiuni SSL noi pe secunda in perioadele de trafic de varf.

# 5. Cerințe privind subcomponentele soluției Centru de Apel MAE

## 1. Portalul

Principalele caracteristici ale acestei zone sunt:

- Servicii de informare si consultanta diferențiate pe zone geografice, în funcție de meridian, limbă sau comunități
- Implementare de noi canale de comunicare (e-mail, blog, forum)
- Asistența specializată din partea unui personal dedicat pe toate aceste canale de comunicație
- Posibilități de interconectare cu alte servicii electronice ale beneficiarului ce vor fi dezvoltate
- Servicii specifice si de interes comunităților – domenii de munca, evenimente/ divertisment, propuneri de colaborare, schimb de informații/ experiență etc

Servicii de preluare/ emitere diferite documente de interes pentru cetățeni

- Această componentă permite gestionarea si afișarea de continut cu privire la informare și consultanță pentru cetățenii români aflati în străinătate, în cadrul zonei publice a sistemului, precum și funcționalități de blog/ forum
- Interfata va fi prevazuta cu un link care permite deschiderea automata a unui form de e-mail in vederea trimiterii de cereri/ sesizări direct din interfată
- Interfata va dispune de posibilitati de interconectare cu alte servicii electronice ale beneficiarului ce vor fi dezvoltate
- Cetatenii romani vor putea deschide cazuri (tichete), folosind formularele web puse la dispozitie de interfata, in functie de tipologia problemei raportate.
- Sistemul va oferi utilizatorilor functionalitati de cautare a tichetelor in functie de numarul de tichet si in baza datelor de autentificare a acestora.

## 2. Componenta front-end web de balansare a încărcării

Componenta front-end web trebuie să asigure:

- Mecanisme de SSL offloading in cazul securizarii comunicatiei client/server fara a aloca resurse de procesate pentru criptare/decriptare la nivelul server-ului de aplicatii
- Reducerea incarcarii server-elor de aplicatii prin mecanisme de cache-ing al continutului de tip static
- Reducerea traficului client/server prin mecanisme de compresie a continutului
- Distribuirea incarcarii provenita de la cererile simultane ale clientilor catre mai multe server-e de aplicatii
- reducerea numarului de IP-uri publice in cazul existentei mai multor server-e de aplicatii.
- Integrarea cu echipamente specifice de accelerare a operatiunilor criptografice cu chei asimetrice (HSM)
- Realizarea unui numar de cel putin 300 de sesiuni SSL noi pe secunda in perioadele de trafic de varf.

Componenta front-end web trebuie să funcționeze în regim de inalta disponibilitate.

Fiecare din elementele constitutive ale componentei front-end web va fi prevazut cu câte un modul hardware pentru suport criptografic destinat operatiunilor specifice SSL.

Cerintele tehnice minime indeplinite de acest modul sunt urmatoarele:

- asigura generarea si procesarea cheilor in hardware;
- asigura, exclusiv pentru utilizatorii autorizati procesarea transparenta a criptarii si decriptarii, respectiv a rutinelor de amprentare criptografica si/sau de semnare digitale in hardware;
- proceseaza nativ rutine de cifru asimetric, respectiv pe baza de algoritmi standard:
    - DSA;
    - Diffie-Helman;
    - RSA (512-4096bit);
    - ECDSA (512bit).
- proceseaza nativ rutine de cifru simetric, respectiv pe baza algoritmilor standard:
    - AES 256;
    - 3DES.
- proceseaza nativ rutine de amprentare criptografica si de certificare de integritate, pe baza algoritmilor standard:
    - SHA-1;
    - SHA-256;
    - SHA-512;
    - RIPEMD160.
- asigura un nivel adecvat de performanta tipica:
    - (minim) 200 de operatii de executare de semnatura RSA cu chei de 1024bit pe secunda;
    - scaleaza natural in configuratii multicomponenta.
- permit asigurarea nivelului dorit de continuitate operationala si de distributie de sarcina, respectiv:
    - suporta mecanisme specifice de echilibrare de sarcina, cum ar fi distributia intre noduri identice, la nivel de sistem de operare, si preluare de sarcina (fail-over) la nivel de aplicatie.
- implementarea componentelor criptografice ale acestor module vor fi certificate, respective cel putin:
    - FIPS 140-2 Level 3.

Se vor include in oferta echipamente criptografice tip HSM, in configuratie identica, din care sa rezulte un numar de 6 partitii criptografice.

## 3. Centrul de preluare a apelurilor dotat cu IVR (CallCenter)

### 1. Cerințe tehnice generale

Sistemul de Call Center va îndeplini următoarele cerințe minime:

Va fi implementat in configurație redundanta cu 2 noduri, in arhitectura activ-activ, bazat pe tehnologia “virtual machine fault tolerant, level 3 ” sau echivalent, asigurându-se astfel că nu vor exista intreruperi ale funcționării aplicatiilor, permitand centrului de preluare a apelurilor o disponibilitate de 100% a tuturor componentelor.

Centrul de preluare a apelurilor va avea urmatoarele componente:

- IVR – Interactive Voice Responder;
- ACD – Automatic Call Distribution;

- Cozi de apeluri;
- Aplicatii operatori/supervizori;
- Sistem de raportare;

Toate componentele sistemului de Call Center (hardware şi software) trebuie sa se integreze între ele, să fie de la acelaşi producator, să nu fie de tip EoS (End of Sales), EoL (End of Life) sau refolosite (Refurbished). Nu se accepta componente de tip "OEM" (Original equipment manufacturer) chiar daca acestea sunt certificate de catre producator pentru componentele considerate critice ale sistemului: servere call center si aplicatia de call center

Componentele sistemul ofertat trebuie sa se integreze din punct de vedere functional cu centrala telefonica a sistemului de comunicatii ofertat. Integrarea trebuie să fie in proportie de 100% la urmatoarele niveluri (se vor prezenta documente explicative semnate si stampilate in acest sens, provenite de la producator):

- baza de date cu utilizatori comună; informaţiile despre utilizatori – nume utilizator, parola, extensie telefonică se vor actualiza în mod unidirectional si în timp real, de la centrala telefonică IP de la misiune la centrala telefonica IP a callCenter-ului si la serverul de CallCenter;
- rutarea apelurilor in functie de apelant si facilitatile agentilor
- controlul unic al operatiunilor legate de apeluri ("call answer", "call transfer", "conference", "call drop", "dialing", "recording", "posibilitate de apelare", "pauze") din fereastra de agent, in acest sens telefonul va fi controlat din aplicatie.

Sistemul de operare pentru cele doua serverele de Call Center ofertate trebuie să fie la ultima versiune comercială de pe piaţă si să facă parte din categoria sistemelor de operare consacrate, exemplu: MS Windows EE, distributii Linux de tip enterprise etc, având suport de la producator (nu se vor accepta versiuni de sisteme de operare fără existenta suportului de la producator).

Hardware-ul ofertat pentru server-ul de CallCenter trebuie sa fie dedicat, nefiind inclus in solutia de tip blade ceruta pentru celelalte componente ale sistemului.

## 2. Cerinţe specifice aplicaţie de Call Center

Arhitectura sistemului de Call Center livrat trebuie să fie redundantă (2 noduri), in mod activ-activ, bazată pe tehnologia "virtual machine fault tolerant, level 3 ". Trebuie să asigure integrare pentru partea de identificare apel si partajare de date cu aplicaţia web de CRM/Ticketing in format standard, descrisa la punctul urmator.

Arhitectura software a aplicatiei de Call Center va asigura obligatoriu urmatoare componente:

- Rutare flow Call Center in functie de:
    - Apelul telefonic si identitatea lui (Inbound)
    - Email routing
    - Skill base routing
    - Identification routing
- Rutare flow apel
    - In functie de data si ora sistemului si apelantului
    - Identitatea apelantului
    - Automated Attendant

    - Coada de asteptare
    - Aplicatia de CRM/Ticketing
    - Voice Mail
- Monitorizare
    - Pentru intreg sistemul
    - Alarme
    - Floor plan
    - Reporting
    - Call Recording
    - Dash board
    - Statistica real time
- Unified communication
    - Colaborare si prezenta
    - Instant messaging
    - Company & External & Web Directory
- Integrare
    - Aplicatia de CRM/Ticketing
    - Baza de date
    - Email – Outlook

## 3. Scalabilitate si echipare Call Center

- Numar total Servere conform specificatiilor: 2
- Numarul total de agenti care trebuie sa fie suportati de Call Center fără adugare de alte componete hardware in configuratia serverelor, este de 500; echipare actuala 10;
- Numarul total de supervizori care trebuie să fie suportati de Call Center 16; echipare actuala 1;
- Numarul total canale IVR simultane care trebuie sa fie suportate de Call Center este de 96; echipare actuala 40 canale simultane.
- Panou de afişare luminos cu minim 20 caractere pentru vizualizare informatii minimale oferite de wallboard.

## 4. Facilități pentru agenți și supervizori:

Sistemul de distribuitie Call Center, ACD (automatic call distribution) si IVR va avea urmatoarele facilități obligatorii pentru agenti și supervizori:

- Să asigure distribuirea apelurilor către agenți.
- Fiecare agent va avea instalat pe PC un software (agent desktop) si sistem de operare consacrat, exemplu: MS Windows, distributie Linux etc, care să îi permită gestionarea apelurilor, si să îi furnizeze informații despre apelul curent (informatii despre apleant: telefon, nume, email, tara - daca exista in baza de date), numărul de apeluri în aşteptare, etc.
- Sistemul trebuie să permită rutarea apelurilor în funcție de diferiți parametri, cum ar fi numărul apelantului, numărul apelat, ora/data, informațiile introduse de apelant in IVR dar si in functie de cozile de asteptare existente si identitatea apelantului;
- Sistemul trebuie să permită rutarea în funcție de informațiile existente în baze de date externa/interna/aplicatia de tip CRM

- Alegerea agentului care va primi apelul trebuie să poată fi făcută atât în funcție de încărcarea acestuia existand mai multe criterii de selectie – cel mai putin utilizat agent, agentul cu cea mai mica medie de timp petrecuta in rezolvarea cazurilor sau selectia circulara a agentilor - cât şi de pregătirea acestuia într-o anumită problema (skill routing).
- Trebuie să existe posibilitatea ca anumite apeluri să poată fi prioritizate în funcție de numărul apelantului sau de informațiile introduse de acesta în IVR, prin introducerea unui PIN cu minim 9 caractere.
- ACD-ul din sistemul de comunicatii trebuie sa faca distribuirea apelurilor catre telefoanele din Call Center in modul fail over pentru aplicatia de Call Center
- Dupa finalizarea apelului telefonic fiecare agent are obligatia de a identifica convorbirea printr-un status predefinit ( „call tagging") in functie de rezultatul cu care considera el ca s-a finalizat conversatia (call type)
- Atunci când considera ca este necesar, agentul trebuie să aibă posibilitatea să înregistreze convorbirea care sa poata fi apoi ascultata de catre acesta sau de catre Supervizor.
- Agent desktop-ul va permite integrarea cu aplicațiile (Windows-based/web-based) folosite de agenți, precum şi definirea unor fluxuri de activități care trebuie executate de către agent în momentul preluării apelului, pe parcursul convorbirii sau la sfârşitul acesteia, folosind o interfață web browsing.
- Agent-ul să dispună de autentificare simplă, de vizualizare în timp real a duratei apelului, si a listei ultimelor apeluri recepționate.
- Modificarea perechii agent-grup de competenta trebuie sa aiba loc instantaneu fara intreruperea sistemului
- Aplicația „Desktop Agent" va oferi suport atât pentru integrarea cu servicii de prezență astfel incat agentul sa aiba usor posibilitatea sa isi defineasca pauze, cât si pentru integrarea cu aplicatia client de e-mail.
- Integrarea „Agent e-mail" va facilita crearea de raspunsuri standardizate ca urmare a cererilor adresate astfel incat sa se poata asigura un control al calitatii in cazul acestui tip de interactiune(e-mail) si sa permita formarea unor cozi de mesaje si routarea acestora catre persoanele competente in oferirea celui mai bun raspuns, astfel incat sa existe un echilibru intre activitatile de preluare de apeluri si activitatile legate de furinzare de raspunsuri sub forma de e-mail.
- Agent-ul telefonic să dispună de software CTI (Computer Telephony Integration) de desktop care asigură comenzile de apelare pentru un telefon IP ( hold – muzica, conferencing – in timp ce clientul este pus pe hold să poată vorbi cu alt agent sau cu supervisorul, transfering – să transfere apelul spre alt agent, chat între agenți şi supervisor, rapoarte cu apelurile anterioare şi cele în desfăşurare).
- Agent-ul trebuie să poată realiza o îmbinare între apelurile inbound şi cele outbound prioritate fiind cele de inbound
- Call back in coada de asteptare, daca unul dintre apelantii la call centere opteaza pentru acesta facilitatate, aplicatia de call center va apela automat acest apelant care a aplicat pentru acesta optiune si-l va distribui agentului de call center disponibil.
- Pentru facilitatea de email routing, se vor defini raspuns automat la email intr-un timp specificat de catre Supervisor in functie de gardul de excaladare a cerintei.
- Supervizorul in cadrul Call Center-ului va avea urmatoarele facilitati/atribuitii:
    - creaza, modifica, sterge si adauga unui grup agentii;
    - asigura sau da facilitati unor anumiti agenti;
    - vizioneaza apelurile in timp real printr-o interfata grafica cu informatii complete
    - monitorizeaza cozile si apelurile in timp real via dashboard, wallboard sau floor plan
    - genereaza rapoarte: imediate si programate cu posibilitate de export pe email sau sub

forma grafica, in functie de diferiti parametri: performanta agentilor, marimea cozii de astptare, numarul de apeluri efectuate/agent, numarul de apeluri pierdute/agent/grup, durata aplelului, etc.
    - defineste tipurile de alarme si actiuni in functie de: marimea cozii de asteptare, numarul de agenti disponibili, durata conversatiei, durata pauzelor pentru agenti, timpul de raspuns, service level, apeluri abandonate, raspusul la email-uri.
- Supervizor-ul să dispună de un program care monitorizează activitatea agenților. Trebuie să poata sa vorbească cu agentii telefonic  sau prin mesaje scrise (chat) şi să transfere apelurile de la un agent la altul, să poată trimite un mesaj text instant către agenți sau grupuri de agenti.
- Un număr arbitrar de agenți trebuie să poată fi definiți ca supervizori şi vor putea folosi un software suplimentar de monitorizare si supervizare. Acest software trebuie să permită monitorizarea agenților şi a cozilor de aşteptare, raportări in timp real, etc. Un supervizor trebuie să poată monitoriza (asculta) un agent(acesta poate fi anuntat sau nu ca este monitorizat de supervizor) în timpul unei convorbiri şi să poată interveni cu indicații pentru agent care să nu fie auzite de către apelant si de asemenea sa poata schimba starea curenta a unui agent (Disponibil, Ocupat, Deconectat)
- Supervisor-ul trebuie să dispună de monitorizare/gestiune stare agenți, grupuri, cozi de aşteptare prin display-uri in timp real, ascultare apel in timp real cu posibilitatea de a interveni,– monitorizare sistem, grupuri, cozi de aşteptare, apeluri şi agenți.
- Supervizorul trebuie sa aiba posibilitatea de a realiza planificarea in interiorul contact center-ului pe o anumita perioada de timp tinand cont de disponibilitatea agentilor, de volumul de apeluri, de expertiza necesara pentru rezolvarea unor situatii specifice, etc.

## 5. Cerințe subcomponenta IVR

- Subcomponenta de raspuns vocal interactiv (IVR) trebuie sa ruleze pe acelasi server cu aplicatia de Call Center si permite formarea cozilor de asteptare pentru ramurile/grupurile de agenti. La achiziție sistemul trebuie să permită minim 40 de apeluri simultane, iar ulterior trebuie să existe posibilitatea de extindere pana la cel putin 90 linii. Numarul de ramuri maxim trebuie sas fie nelimitat si sa depinda exclusiv de resursele serverului pe care se instaleaza componenta.
- Subcomponenta trebuie să ofere o interfață grafică uşor de utilizat care să permită definirea de scripturi de interacțiune cu utilizatorul, culegerea de informații de la acesta (prin DTMF), căutări de informații în baze de date.
- Subcomponenta trebuie să ofere o aplicatie separata si independenta pentru Supervisor si Administrator in care Administratorul sistemului da facilitati Supervizorilor.
- Subcomponenta trebuie să ofere meniuri vocale predefinite care să ofere clientului posibilitatea alegerii unei acțiuni prin apăsarea tastelor asociate
- Subcomponenta trebuie sa ofere apelanților în aşteptare opțiuni IVR (promo, muzică), fără pierderea poziției în coada de aşteptare
- Meniul vocal interactiv să răspundă la apeluri 24 de ore din 24, cu mesaj de întâmpinare personalizat şi să direcționeze apelurile către persoane, departamente.
- Subcomponenta trebuie sa ofere un modul de direcționare poate include niveluri multiple, astfel încât apelanții pot alege singuri destinația dorită in functie de PID,limba etc.
- Subcomponenta IVR va fi redundanta, asa cum este prevazut si intreg sistemul de Call Center si va rula pe aceeasi masina(server) ca si aplicatia de Call Center
- Inregistrarea mesajelor în cadrul meniurilor vocale interactive trebuie să poată fi făcută în format audio standard si sa se poată folosi orice Sound Recorder.

- Subcomponenta trebuie sa puna la dispozitie scripturi cu scop informativ pus la dispoziția cetățeanului in limba romana obligatoriu plus alte cinci limbi internationale, cu ocazia diferitelor evenimente, în care apelurile telefonice sunt preluate de meniuri vocale interactive extinse, cu posibilitatea redirectării către agenți.
- Subcomponenta trebuie sa ofere posibilitatea de integrare cu aplicatii third-party de tipul email-to-fax.

# 4. Sistem de gestiune a tichetelor (Componenta colaborativa tip CRM)

## 1. Cerinte functionale generale

- Sistemul va permite definirea de modele informaționale care să gestioneze tipurile de date folosite și modul în care acestea relaționează, fără interventia furnizorului, fără a scrie cod sursa suplimentar și fără a afecta datele existente în cadrul sistemului.
- Sistemul va permite căutarea în baza de date folosind diferite filtre și criterii ce vor fi definite de către utilizatori, fără limitări asupra posibilităților de filtrare a informațiilor; practic, căutarea în baza de date se va efectua în funcție de orice entitate sau relație din cadrul modelelor informaționale, predefinită sau definită de utilizator și prezentă în aplicație la momentul căutării
- Sistemul va dispune de o componenta de analiza care va putea fi configurata in functie de modelele informationale create, fara interventia furnizorului, fara a scrie cod sursa suplimentar si fara a afecta datele colectate deja in baza de date
- Sistemul va permite utilizatorilor sa defineasca reguli de business specifice in vederea identificarii diferitelor scenarii intr-un anumit scop, de exemplu, pentru a valida datele introduse in sistem prin modulele de introducere de date - daca utilizatorul introduce date gresit sau intr-un format neacceptat, sistemul va afișa mesaje de infomare indicând acest lucru precum și faptul că datele nu pot fi transmise la server până la efectuarea corecțiilor
- Sistemul va permite utilizatorului definirea de reguli care pot identifica doua instante ale unei entitati ca fiind identice. De exemplu, o persoana poate raporta in diferite scenarii (diferite xml-uri), eventual provenind din surse diferite. In baza unei reguli de deduplicare definita de utilizator, folosind atribute specifice acesteia, sistemul poate identifica persoana ca fiind aceeasi cu alta inregistrata in alte scenarii.
- sistemul va permite inregistrarea de catre operatori a cazurilor (tichetelor) preluate prin apeluri telefonice, gestionarea efectiva de catre operatori a tuturor tichetelor inregistrare in cadrul sistemului (managementul cazurilor) si definirea integrarii fluxurilor de lucru in cadrul sistemului
- Un tichet (caz) poate fi creat/ definit prin urmatoarele componente:
    - Prin Portal: inregistrare directa sau folosirea link-ului in vederea trimiterii de e-mailuri
    - Prin Call Center: preluarea apelului telefonic de catre operator, deschiderea tichetului in cadrul sistemului de catre operator si anexarea inregistrarii convorbirii telefonice
- In functie de etapa din cadrul fluxului pe care se incadreaza un tichet la un moment dat, sistemul trebuie sa permita existenta mai multor stari/stadii aferente tichetului respectiv: „nou”, „in curs de solutionare”, „rezolvat” etc. Nomenclatorul complet al stadiilor posibile pentru un tichet se va completa in faza de analiza. Schimbarea starii pentru un tichet se va efectua in functie de evenimentele interne din cadrul fluxului de lucru al sistemului
- Sistemul va oferi operatorilor sistemului functionalitati de cautare a tichetelor in functie de numarul de caz si alte criterii avansate de cautare, configurabile in functie de metadatele ce

urmeaza a fi identificate in etapa de analiză

- Sistemul va permite efectuarea de cautari aproximative prin implementarea unui mecanism complex de cautare si analiza de cuvinte, folosind un algoritm de identificare a unei entitati in baza informatiilor partiale, inclusiv a celor partial eronate – atunci cand cautarea exacta nu intoarce niciun rezultat.
- Sistemul va permite „arhivarea" unui tichet la inchiderea acestuia, prin scoaterea sa din zona curenta de lucru si incadrarea in cadrul zonei de tichete arhivate.
- Tipologia fluxurilor din cadrul sistemului include:
    - Fluxuri generate de un tichet nou
    - Fluxuri interne de lucru ale operatorilor
    - Fluxuri de autentificare a utilizatorilor
    - Fluxuri de generare/ gestionare de documente aferente unui tichet
    - Fluxuri de comunicare a rezultatelor si trimitere de notificari.
- Sistemul va permite definirea de fluxuri operaționale a tichetelor în vederea dispecerizării şi prelucrării acestora în termene cât mai scurte şi de o manieră controlabilă. Pot fi pornite fluxuri ad-hoc si predefinite de tip informare/distribuire sau de tip avizare/aprobare cu selectarea operatorilor care vor fi implicați.
- Sistemul va permite crearea de fluxuri prin intermediul unui editor grafic specific, folosind interfata web a aplicatiei, fara a fi necesara scrierea de cod sursa
- Sistemul va permite implementarea mai multor fluxuri de activitati in paralel, iar notificarile/alertele aferente acestora sa poata fi trimise pe e-mail;
- In fiecare stadiu al unui flux, o persoana sau un grup de persoane are responsabilitatea pentru o anumita sarcina/ un anumit document.
- Sistemul trebuie să implementeze următoarele obiecte aferente fluxurilor:
    - Initierea
        - Manuala - Un flux poate fi initiat manual de catre un utilizator al sistemului care are drepturi adecvate.
        - Programator activitati - Utilizatorii pot defini programari pentru initierea automata a unor anumite fluxuri.
        - Tichet creat - Un flux poate fi initiat la crearea unui nou tichet.
    - Actiuni fluxuri
        - Start - Pas generic care marcheaza punctul de inceput in cadrul fluxului.
        - Stop - Pas generic care marcheaza finalizarea unui flux
        - Decizie bazata pe regula - Acest tip de pas este folosit pentru definirea unei reguli formale bazate pe atributele unui document, status flux sau variabile flux, etc si permite luarea unei decizii referitoare la urmatorul pas din cadrul unui flux.
        - Setarea atributelor entitatilor - Acest tip de pas este folosit pentru setarea atributelor unei entitati din cadrul unui flux cu o anumita valoare – de exemplu schimbarea statusului unui tichet la solutionarea acestuia.
        - Stabilirea statusului fluxului
        - Stabilirea variabilelor de flux
        - Crearea notificarilor
    - Sarcini in cadrul unui flux - Sarcinile reprezinta activitati care trebuie finalizate intr-o anumita perioada de timp, avand anumiti responabili.
    - Notificari - Notificarile reprezinta mesaje predefinite transmise de sistem, avand urmatoarele atribute:
        - Subiect/Text

        - Modalitate transmitere: Email
        - Destinatar
    - Obiecte custom – contin toate tipurile de obiecte si atribute definite de utilizator

- Sistemul trebuie să implementeze următoarele operațiuni de gestiune a tichetelor:
    - Deschiderea unui tichet :
        - Deschiderea tichetului ca urmare a unui apel telefonic
        - Deschiderea unui tichet in urma inregistrarii acestuia pe portal
        - Deschiderea unui tichet ca urmare a unui mesaj electronic
    - Actualizarea unui tichet
        - Actualizare tichete pe baza informatiilor obtinute din knowledgebase
        - Actualizare tichet pe baza informatiilor obtinute din sisteme externe
        - Actualizare tichet cu informatii care concluzioneaza cazul
    - Inchiderea unui tichet
        - Procedura de inchidere
        - Procedura de diseminare a rezultatului
    - Arhivarea tichetului
        - Mutarea tichetului intr-o zona de arhiva, in afara spatiului de lucru uzual

## 2. Cerințe specifice de personalizare a soluției

- Solutia trebuie sa permita modalitati de integrare prin WebServices.
- Solutia trebuie să conțină un modul web de customizare a interfetei utilizator prin adaugarea de noi entitati, noi atribute in baza de date, publicarea atributelor pe forme, definirea de noi relatii intre entitati
- Solutia trebuie sa permita adaugarea din interfata web a urmatoarelor tipuri de atribute: varchar, nomenclator – picklist, int, money, date and time.
- Solutia trebuie sa permita integrarea cu alte aplicatii web prin functionalitati de tipul IFRAME – cu transmiterea de parametri (cel putin a identificatorului unic de inregistrare).
- Sa permita setarea atributelor in urmatoarele variante: fara constrangeri, sau obligatoriu de completat.
- Solutia trebuie sa permita adaugarea prin interfata web a scripturilor (javascript) care sa personalizeze interfata in functie de modificarea valorii unui camp din forma.
- La introducerea unei noi entitati din interfata web solutia trebuie sa aibă facilitatea de setare a posibilitatii de a permite atasamente asociate inregistrarilor pentru entitatea in cauza.

## 3. Cerințe specifice legate de baza de cunostințe (knowledgebase)

- Solutia de gestiune a tichetelor trebuie sa includa functionalitati de tip knowledgebase.
- Solutia trebuie sa permita definirea de template-uri de articole knowledgebase cu functiile standard de formatare (bold, italic, underline, etc).
- Componenta de tip knowledge base trebuie sa contina un motor de cautare dupa diverse functii: cuvinte cheie, fraze, titlu, continut, numar de articol.
- Utilizatorii cu drepturi specifice trebuie sa poata introduce noi persoane in baza de date.

- Solutia trebuie sa permita inregistrarea unui numar nelimitat de adrese pentru o persoana.
- Solutia trebuie sa permita inregistrarea unui numar nelimitat de sesizari pentru o persoana.
- Inregistrarile de tip persoana trebuie sa poata fi atribuite unui teritoriu.
- Pe fiecare inregistrare de tip persoana trebuie sa fie vizibil istoricul interactiunilor cu acesta si istoricul sesizarilor.

### 4. Cerințe specifice pentru managementul instituțiilor

- Solutia de gestiune a tichetelor trebuie sa permita administrarea institutiilor care ofera suport in rezolvarea sesizarilor. Inregistrarile de tip institutie trebuie sa poata fi configurate astfel incat sa contina parametrii necesari in vederea escaladarii sesizarii.
- Inregistrarile de tip institutie trebuie sa contina informari referitoare la adrese de contact, numere de telefon, descrierea responsabilitatilor, etc.
- Solutia trebuie sa permita inregistrarea unui numar nelimitat de adrese.
- Solutia trebuie sa permita inregistrarea unui numar nelimitat de persoane de contact pentru o institutie.
- Solutia de suport informational trebuie sa permita clasificare institutiilor pe tipuri si structurare geografica a acestora.

## 5. Componenta de analiză și raportare

- Sistemul trebuie să includă o componentă de analiză a informațiilor centralizate în baza de date, bazată pe mecanisme specifice solutiilor software de tip Data Warehouse si cele de suport decizional (business inteligence), componentă care va putea identifica aspecte de interes pentru Beneficiar în funcție de modelele informaționale definite.
- Sistemul trebuie să ofere posibilitatea intocmirii de rapoarte in baza informatiilor din baza de date. Rapoartele pot fi atat predefinite cat si configurate de utilizator si pot prezenta datele in diferite formate: tabelare, grafice de diferite tipuri.
- Sistemul trebuie să dispună de mecanisme care sa permită:
    - definirea regulilor de business necesare determinarii zonelor geografice cu un risc ridicat determinat in raport cu o cauza specifica;
    - identificarea tuturor cazurilor asociate unei anumite cauze si stabilirea de legaturi intre cazuri in functie de anumiti parametri, de exemplu regiunea in care se raporteaza
    - cautarea in baza de date de analiza folosind filtre si criterii de cautare specifice in functie de entitatile folosite cat si mecanisme de cautare avansata.
    - obtinerea de statistici pe baza analizei informatiilor din baza de date si construirea de rapoarte configurabile pe baza acestora
    - prezentarea datelor din sistem sub formă de analiză in functie de mai multe criterii predefinite – rapoarte configurabile
    - prezentarea datelor din sistem sub forma de rapoarte definite ad-hoc prin selectarea de catre operator a parametrilor de afisare (dimensiuni si măsuri)
    - afisarea datelor din sistem sub forma de graf de relații cu posibilitatea de plasare pe harta a anumitor zone geografice, considerate de risc ridicat in functie de incidenta tichetelor (cazurilor) raportate si identificarea riscurilor specifice unor anumite zone geografice.

- analiza vizuala a informațiilor prin crearea și analiza grafurilor, având ca fundament informațiile din baza de date. Componenta de analiza vizuala va colecta informatiile din baza de date si le va afisa in diferite forme vizuale.
- generarea automata a unor rapoarte in baza unor programari predefinite
- crearea si analiza grafurilor avand ca fundament informatiile din baza de date, precum si calcularea de diferite metrici in baza informatiilor stocate in cadrul bazei de date.
- adaugarea de noduri si relatii atat prin importarea din baza de date cat si manual, prin metoda "drag and drop"

- Sistemul trebuie să pună la dispozitie mecanisme de:
  - editare a grafurilor definite
  - calculare a metricelor, spre exemplu: Centralitate Betweeness si Centralitate Closeness
  - afisare a datelor in forme vizuale diferite, spre exemplu: manuala, arbore, automata, in adancime, circulara, matriciala, temporara etc.
  - descoperire a relatiilor dintre entitati plecand de la structurile existente sau de la gradul de aparitie al unor scenarii
  - Gestionare a grafurilor.
- Afișarea datelor din sistem va fi efectuata:
  - după criterii predefinite – rapoarte predefinite
  - prin rapoarte la cerere / existența unui mecanism la îndemâna utilizatorilor de a introduce noi date în rapoartele predefinite si a modifica structura unui raport adhoc prin selectarea si filtrarea dimensiunilor si a masurilor asociate unui cub multidimensional
  - sub formă de graf / geospațial (incidența cazurilor pe regiuni, pe tipuri de cauze, depistarea aceleiași cauze)
- Afișarea utilizării sistemului, încărcarea pe operatori va fi efectuată:
  - dupa criterii privind tipurile de cazuri definite in sistem
  - dupa criterii privind utilizatorii si/sau grupurile din care fac parte utilizatorii si/sau grupurile din care fac parte utilizatorii si/sau grupurile din care fac parte utilizatorii in sistem
- Rapoartele de utilizare a sistemului trebuie sa permita obtinerea informatiilor grafic si numeric. Sistemul de raportare trebuie sa permita generarea de rapoarte ad-hoc in sistem grafic si numeric pe baza criteriilor definite de catre utilizatori.

## 6. Componenta de gestiune a identității utilizatorilor MAE

- Proiectul se adresează atât cetățenilor cât şi personalului Ministerului Afacerilor Externe. Personalul implicat în desfăşurarea proiectului va avea roluri distincte după cum urmează:

**Rolul A:Operator** Centru de Contact şi Suport pentru Cetățenii aflați în străinătate –minim 40 de persone. Operatorii vor realiza următoarele activități:

- preluare apeluri telefonice şi sesizări electronice din portal, respectiv email-urile cetățenilor;
- prin aplicația colaborativă de tip CRM vor deschide tichetul/cazul;
- vor prelua informațiile necesare identificării solicitantului şi le vor ataşa tichetului/cazului;

- vor analiza situația descrisă şi o vor cataloga în vederea soluționării;
- vor transfera tichetul/sesizarea către un responsabil MAE abilitat, în momentul în care cazul depăşeşte competențele operatorului;
- vor urmări şi vor închide tichetele/cazurile când acestea vor fi rezolvate.

**Rolul B: Supervizor** al echipei de operatori Centru de Contact şi Suport pentru Cetățenii aflați în străinătate: minim 1 - maxim 4 persoane. Supervizorii operatorilor din Centrul de Contact vor avea urmatoarele responsabilități:

- vor organiza echipele şi turele pentru ca operatorii să asigure funcționarea centrului de contact 24 de ore, 7 zile pe săptămână;
- vor supraveghea buna desfăşurare a activităților din centrul de contact;
- vor asigura suport operatorilor în cazurile cu grad ridicat de dificultate;
- vor urmări soluționarea tichetelor/cazurilor deschise de către operarori şi transferate responsabililor abilitați MAE;
- vor escalada către superiorii ierarhici (director direcție, consul, consul general etc) situațiile excepționale, cazurile de întârziere a soluționării tichetelor/cazurilor transferate sau alte situații specifice;
- vor întocmi rapoarte lunare/trimestriale privind activitatea centrului de contact, situații cu cazuistica semnalată şi soluțiile propuse;
- vor propune idei de îmbunătățire a activităților şia fluxurilor de lucru cu cetățenii.

**Rolul C: Administrator sistem**: minim 1 - maxim 3 persoane. Administratorul de sistem va asigura:

- mentenanța sistemelor care asigură funcționarea centrului de contact şi suport în regim 24 ore, 7 zile pe săptămână;
- managementul utilizatorilor şi a accesului la informațiile ce rezultă în urma activităților desfăşurate în cadrul centrului de contact şi suport;
- sprijin Operatorilor şi Supervizorilot acestora în cazul unor dificultăți tehnice;
- administrareaaplicațiilor şi accesului la informații;
- instruirea Operatorilor nou-veniți în vederea utilizării sistemelor.

**Rolul D: Management**: minim 10 - maxim 140 persoane. Personalul aflat pe poziții de conducere în cadrul Ministerului Afacerilor Externe şi al reprezentanțelor diplomatice va avea acces la aplicațiile solicitate în cadrul proiectului în baza unei solicitări care va fi validată pe fluxul de aprobari din cadrul Ministerului Afacerilor Externe. Managementul din cadrul MAE va putea analiza rapoartele de activitate, propunerile pentru îmbunătățirea activităților şi fluxurilor şi pot dispune asupra acestora.

- În proiect se va oferta o soluție integrată de management al identității care va acomoda rolurile de mai sus, fără a se limita la acestea.

## 1. Obiective generale ale componentei de gestiune a identitatii utilizatorilor MAE

- Automatizarea ciclului de viata al utilizatorilor in sensul crearii, modificarii si stergerii acestora din sistemele de networking, email, baze de date, etc.
- Administrarea tuturor identitatilor pentru angajati si, posibil, pentru utilizatorii externi.
- Furnizarea unui modul de auto-administrare prin care utilizatorii pot cere acces la diverse

resurse si acestea sa fie aprobate de roluri predefinite (roluri ce permit accesul la resurse predefinite).
- Furnizarea unei platforme deschise care sa permita conectarea facila a diverselor aplicatii sau sisteme.

## 2. Cerinte Generale

Solutia de management a indentitatii trebuie sa:

- Includa interfete administrative capabile web
- Ruleze ca un site web securizat
- Ofere capabilitatea de a detecta orice schimbare in informatia referitoare la un utilizator (nume, prenume, parola, alte proprietati) care apare in orice sursa care contine respectiva informatie si sa propage in mod automat acea schimbare catre orice alta sursa care contine informatii despre acel utilizator. Mecanismul de propagare trebuie sa fie configurabil.
- Poata prelua informatiile despre utilizator din surse multiple: fisiere neformatate, fisiere XML, baze de date, servere de directoare.
- Fie compatibil cu surse multiple care stocheaza informatiile de identitate (precum un sistem HR, baze de date, fisiere, servere de directoare).
- Ofere capabilitatea de a aloca / modifica drepturile de utilizator / privilegiile de acces la resursele organizatiei in functie de politicile existente in organizatie si de rolul utilizatorului in organizatie.
- Ofere capabilitatea de a delega responsabilitatea de administrare catre divizii, departamente sau alte unitati ale organizatiei
- Ofere capabilitatea de a permite utilizatorilor sa isi administreze parolele, incluzand schimbarea si resetarea parolelor fara interventia administratorilor.
- Permita utilizatorilor sa solicite crearea de noi conturi folosind un browser web.
- Permita utilizatorilor sa isi actualizeze informatiile personale (adresa, telefon etc) si sa propage in mod automat informatia catre toate resursele organizatiei care contin total sau partial acele informatii.
- Contina un motor pentru fluxul de lucru care directioneaza orice cerere catre aprobatorul sau aprobatorii corespunzatori;
- Suporte notificarile trimise printr-un sistem email.
- Ofere o interfata grafica pentru configurarea fluxului de lucru conform politicilor / procedurilor existente in organizatie.
- Ofere capabilitatea de a vizualiza solicitarile oricarui utilizator sau cererile care privesc solicitarile legate de modificarea informatiei utilizatorului.

## 3. Cerinte specifice de administrare a conturilor de utilizator

Solutia de management a identității trebuie sa:

- Asigure ca fiecare cont de utilizator are un ID unic.
- Ofere reguli configurabile pentru crearea identificatorilor unici.
- Permita utilizarea unei date de expirare care poate fi utilizata pentru a urmari innoirea / stergerea / modificarea conturilor de utilizator.
- Suporte expirarea conturilor de utilizator pentru diferite tipuri de utilizatori folosind o data de

expirare a contului sau o data de terminare a contractului

- Permita notificarea prin email a proprietarului oricarui cont care a fost inactiv pentru o perioada configurabila.
- Ofere o politica de revocare/stergere a conturilor inactive in cadrul unei perioade configurabile.
- Ofere capabilitatea de a exporta/importa conturi de utilizator.
- Ofere capabilitatea de a aproba in mod automat orice solicitare printr-un set de reguli si politici.
- Ofere capabilitatea de a vizualiza o solicitare de cont care a fost trimisa si datele asociate cu acea solicitare.
- Permita crearea de reguli bazate pe roluri ale utilizatorilor
- Produsul trebuie sa suporte gestionareade roluri dupa cum urmeaza:
    - Atribuirea utilizatorilor catre mai multe roluri
    - Atribuirea utilizatorilor catre roluri ierarhice
    - Produsul trebuie sa ofere capabilitati de a specifica roluri care exclud alte roluri pentru a preveni atribuirea de roluri care s-ar afla in conflict
    - Asigure atribuirea de propietati pentru contul de utilizator odata cu rolul utilizatorului.
- Permita utilizarea sistemelor de informatii cheie din mediul organizatiei ca sursa de informatii de incredere despre informatii de identitate pentru declansarea automata de conturi (de ex detectarea noilor angajati adaugati si crearea automata de conturi pentru noii angajati in functie de rolul lor in organizatie).
- Permita atribuirea de resurse pentru cont odată cu rolul
- Permita atribuirea,pentru unii utilizatori, de drepturi de acces diferite de cele corespunzatoare rolurilor respectivilor utilizatori.
- Permita atribuirea de drepturi de acces individuale, distincte, pe langa cele definite in cadrul rolului.
- Poate schimba dinamic si automat drepturile de acces in functie de schimbarile din rolurile utilizatorilor.
- Genereaze ID-uri de utilizator unice, in conformitate cu politicile organizatiei.
- Suporte notiunea de „roluri persistente” (adica schimbarile facute definitiei unui rol sunt aplicate tuturor utilizatorilor sub acelasi rol)
- Suporte mutarea unui utilizator dintr-un rol in altul, impactul fiind modificarea drepturilor de acces corespunzatoare noului rol.
- Suporte optiuni multiple de anulare a drepturilor (precum oprirea dar lasarea conturilor intacte, stergerea conturilor dar pastrarea identitatii utilizatorului, sau stergerea cu totul a utilizatorului).
- Suporte descoperirea automata si rezolvarea inadvertentelor de informatii de identitate dispersate pe mai multe resurse (de exemplu, sincronizarea datelor intre mai multe directoare, baze de date si fisiere)

## 4. Cerinte specifice legate de delegarea administrarii

Produsul ofertat trebuie sa:

- Ofere capabilitati de administrare granulara delegata precum politici de informatie interna de control al accesului (ACI) care limiteaza atat accesul utilizatorului cat si al administratorului la rapoarte, informatii ale utilizatorilorsi functii operationale, pentru toate atributele si operatiile de gestiune a identitatii (stergere, transfer, cautare, recuperare, suspendare, adaugare si modificare).
- Ofere abilitatea de a propaga utilizatorii desemnati (administratorii delegati) in functie de rol sau in functie de un set de atribute configurabile

- Permita sarcinilor administrative ‘n‘ niveluri de profunzime
- Fie capabil sa lucreze in medii izolate (retele izolate prin firewall-uri etc.)
- Utilizeze tehnologia internet (email si pagini web) pentru a facilita fluxurile de lucru de aprobare

## 5. Cerinte specifice legate de administrarea parolelor

Produsul ofertat trebuie să:

- Ofere functii de resetare a parolelor conturilor pe platformele administrate
- Sincronizeze parolele pentru utilizatori imediat ce utilizatorul si-a schimbat parola
- Includa o notificare de operatie reusita/nereusita pentru administrearea parolei (resetare si sincronizare).
- Trimita o notificare tip email catre un utilizator intr-o maniera configurabila cu un numar de zile inainte ca parola/contul sau sa expire.
- Poata sa genereze in mod aleator parola initiala a unui cont de utilizator.
- Poata forta utilizatorul sa schimbe parola resetata dupa prima folosire.
- Aiba abilitatea de a impune anumite combinatii configurabile de caractere alfa-numerice intr-o parola.
- Poata impune politica parolei (lungime, nr. caractere alfanumerice, caractere neacceptate etc.) atunci cand utilizatorii schimba sau sincronizeaza parole
- Suporte o lista de parole restrictionate pentru a nu permite utilizatorilor sa selecteze cuvinte comune.
- Poata mentine un istoric al parolelor configurabil pentru a evita reutilizarea parolei.
- Ofere capabilitatea de a genera parole ca un set aleatoriu de numere si caractere cu lungime configurabilla
- Suporte un numar configurabil de intrebari pentru recuperarea parolei in eventualitatea unei parole uitate. Numarul si continutul intrebarilor si raspunsurilor trebuie sa poata fi configurat de catre fiecare utilizator.

## 6. Cerinte specifice legate de fluxurile de lucru automatizate

Produsul ofertat trebuie să:

- Ofere capabilitatea ca oricarui utilizator sa-i fie atribuita o actiune printr-un proces de flux de lucru
- Ofere capabilitatea ca anumiti utilizatori sa aiba privilegii de acces specifice pentru a crea, modifica si/sau sterge un proces de flux de lucru.
- Aiba capabilitatea de a initia procese de fluxuri de lucru bazate pe declansatori veniti din sisteme externe.
- Aiba capabilitatea de a detecta noii angajati adaugati intr-un sistem HR sau in alte surse si automatizeaza procesul de acordare a drepturilor pentru noul utilizator.
- Aiba capabilitatea sa automatizeze procesul de acordare sau luare a drepturilor cu sau fara un flux de lucru.
- Coponenta flux de lucru a produsului trebuie sa fie o functionalitate integrata a produsului.
- Componenta flux de lucru a produsului trebuie sa ofere abilitatea sa ridice nivelul sau sa transmita actiunile/cererile in functie de data la care au fost initiate.

- Componenta flux de lucru trebuie sa suporte cerinte logice continute intre diferite etape.
- Componenta flux de lucru a produsului trebuie sa permita participantilor la fluxul de lucru sa intreprinda actiuni (aprobare / rejectare) prin intermediul unui browser web.
- Componenta flux de lucru a produsului trebuie sa suporte transmiterea solicitarilor folosind sisteme de mesagerie (e-mail).
- Componenta flux de lucru a produsului trebuie sa suporte bifurcatii si impreunari ale proceselor.
- Componenta flux de lucru a produsului trebuie sa suporte crearea unui flux de lucru cu etape multiple si lansarea unui sub-flux de lucru.
- Componenta flux de lucru a produsului trebuie sa suporte procesele care pot avea sub-fluxuri de lucru sau fluxuri gazduite.
- Componenta flux de lucru a produsului suporta reutilizarea proceselor/fluxurilor de lucru create.
- Componenta flux de lucru a produsului trebuie sa suporte transmiterea bazata pe rol catre recipienti.
- Componenta flux de lucru a produsului trebuie sa suporte roluri alternatoare (delegati)
- Componenta flux de lucru a produslui trebuie sa ofere o interfata grafica pentru dezvoltarea proceselor/fluxului de lucru.

## 7. Cerinte specifice pentru modulul de raportare al subcomponentei de gestiune a identității

Solutia trebuie sa ofere următoarele rapoarte standard (incluse cu solutia):

- Raport de operatii – Raport ale tranzactiilor operationale de un anumit tip (de ex. Adaugarea unui nou utilizator)
- Raportul de serviciu – tranzactiile trimise care afecteaza oferirea catre resurse administrate (de ex server al instituției)
- Raport de utilizator – tranzactiile trimise care afecteaza conturile utilizatorilor
- Raport de respingere – conturile respinse de catre aprobatori in cadrul procesului fluxului de lucru
- Raport de reconciliere – rezultatele din reconcilierile recente ale unei resurse administrare
- Raportul conturilor inactive de catre Resursa Administrativa
- Raportul conturilor – listeaza utilizatorii si conturile asociate si daca contul se conformeaza politicilor curente sau nu.
- Rapoartele trebuie sa fie generate in timp real catre utilizator/administrator
- Rapoartele pot fi exportate in format pdf
- Solutia trebuie sa poata genera rapoarte configurabile

## 8. Cerinte specifice pentru interfata cu utilizatorul

Interfata cu utilizatorul trebuie sa fie configurabila, permitand:

- specificarea fonturilor,
- specificarea culorilor,
- numele de afisare ale campurilor,
- amplasamentul siglelor

## 9. Cerinte specifice legate de arhitectura de conectare

Produsul ofertat trebuie să:

- Ofere conexiune fara agenti, in afara de agentii platformei locale catre resurse de administrare
- Ofere agenti/conexiuni catre urmatoarele resurse:
    - Sistemul de operare
    - Servere de aplicatii
    - Sisteme de Directoare
    - Baze de date
    - Produse de autentificare majore
    - User ID/password
    - LDAP
    - Tokens
    - SecurID
    - Smart cards
    - USB key
    - RF badge
    - PKI certificates
    - Biometrics
    - Produse web SSO
    - Platforme de mesaje/email
    - Aplicatii de tip help desk
    - Aplicatii ERP
    - Aplicatii HR
- Includa un SDK pentru a extinde acoperirea platformelor administrate prin aplicatii customizate si proprietare (construite in companie)
- Permita sistemelor externe sa acceseze sau sa interogheze date din interiorul produsului (de ex LDAP, ODBC, JDBC etc)
- Includa un “scheduler” pentru rularea sarcinilor programate

## 10. Caracteristici de securitate specifice solutiei de management al identitatii

Produsul ofertat trebuie sa:

- Foloseasca un mecanism de autentificare LDAP cu nume de utilizator si parola pentru toate tipurile de acces, inclusiv GUI, web si cereri API
- Să se integreze (folosind plugin-uri sau agenti) cu solutia de autentificare a utilizatorilor.
- Poata impune incetarea sesiunii din cauza inactivitatii pe o perioada de timp configurabila
- Permita ca toate parolele să fie mascate la introducere
- Permita ca toate sesiunile de comunicare din solutie sa fie securizate folosindu-se sesiuni de criptare SSL 128 bit. Aceasta cerinta include toate sesiunile utilizatorilor finali cu browsere web precum si comunicarea intre componentele solutiei precum serverul de management si agentii sai.
- Ofere o politică de parola care se poate aplica global tuturor conturilor țintă sau care poate fi atribuită unuia sau mai multor servicii țintă, și are mai multe aspecte, incluzand:
    - Lungime minima si maxima

    - Numarul maxim de caractere repetabile
    - Numarul minim de caractere alfa si/sau numerice
    - Definirea caracterelor invalide si/sau a celor cerute
    - Restrictionarea primului caracter si/sau a intregii parole la un set de caractere declarat
    - Numărul de parole precedente sa nu fie permis (inclusiv cele scrise invers)
    - Nepermiterea numelui de utilizator si/sau a IDului de utilizator ca parola
    - Nepermiterea parolelor găsite în dicționare
- Permita ca valoarea initială a parolei trebuie sa fie limitată la prima folosire
- Ofere posibilitatea de a genera parole aleatoare
- Ofere metodele de suspendare/terminare/modificare a contului in cauza conform politicii organizatiei daca statutul unui utilizator se schimba (schimbarea rolului, schimbarea zonei de responsabilitate, concediu fara plata, terminare etc)
- Ofere metode pentru prevenirea reuitilizarii identitatilor conturilor dupa ce acestea au fost retrase

## 7. Cerinte privind subcomponenta de securitate a sistemului informatic

Subcomponenta de securitate a sistemului informatic trebuie să implementeze o arhitectură web multi-tier care să permită definirea prevederilor de securitate la nivelul urmatoarelor straturi ale aplicațiilor:

### 1. Nivelul Prezentare

Stratul de prezentare cuprinde interfata utilizator si este responsabil cu interactiunea platformei cu utilizatorul realizata prin intermediul tehnologiei standard Internet browser cu capabilitati JavaScript.

Paginile HTML afisate de catre stratul de prezentare sunt generate de catre stratul de aplicatie (business logic). Validarile simple vor fi executate pe masina client prin intermediul JavaScript sau o metodă echivalentă; validarea finală a datelor va fi insa realizata exhaustiv de catre stratul de aplicație.

Din motive de securitate, comunicarea pentru zonele confidentiale se va realiza utilizand protocolul HTTPS, un protocol securizat care ofera servicii de tunelare criptata peste protocolul HTTP. Utilizarea protocolului HTTPS va asigura o comunicare securizata.

Va exista doar un singur punct de autentificare. Utilizatorul va fi autentificat o singura data pe durata intregii sesiuni. Informatiile furnizate de catre stratul de aplicatie vor fi create dinamic – paginile afisate vor prezenta doar acele informatii accesibile utilizatorului curent in functie de rolul desemnat.

### 2. Nivelul Business Logic

Modelul de business logic asigura transparenta complexitatii acestuia fata de utilizatori, fiind organizat conform urmatoarelor principii: standardizare, reutilizare, separare clara intre nivelul de prezentare si business logic , orientare pe servicii.

La acest nivel se vor asigura, din punct de vedere al securitatii, procesele de autentificare si autorizare, managementul sesiunilor utilizatorilor, reguli de validare intrari si integritate date.

Toate datele necesare serviciilor de autentificare si autorizare sunt stocate în baza de date pentru utilizatori, optimizata corespunzator (directory services) pentru a permite un timp de raspuns minim. In acest sens, toate subsistemele platformei vor comunica la acest nivel cu un server LDAP (Lightweight Directory Access Protocol).

Acest protocol va fi folosit de catre serverele de aplicatie pentru a comunica cu alte baze de date in cadrul proceselor de autentificare si autorizare. Accesul la baza de date LDAP va fi restrictionat conform unor nivele de acces bazate pe seturi de permisiuni.

Utilizarea LDAP va permite o administrare centralizata a soluției de securitate propusă, ce cuprinde elemente precum conturi de cursant, instructor, administrator, parole, nivele de acces etc. La nivel global, pentru toate subsistemele.

Stabilirea unei sesiuni de lucru consta in operatiunea de autentificare (login) a utilizatorului curent.

Operația de autentificare este realizata o singura data pe sesiune (single sign-on). Sesiunea curenta este invalidata prin operatia de terminare a sesiunii ceruta explicit de catre utilizatorul curent, sau prin expirarea timpului de sesiune.

Autentificarea utilizatorilor la nivelul aplicatiilor de Portal si CaseManagement trebuie sa permita utilizarea dispozitivelor criptografice prevazute; de asemenea este necesara verificarea online a statutului certificatelor utilizatorilor in cadrul procesului de autentificare prin folosirea protocoalelor specifice:OCSP si CRL.

Procesul de autorizare consta in filtrarea tuturor solicitarilor de servicii in baza permisiunilor asociate sesiunii curente. Restrictiile de acces pot fi individualizate printr-un set de privilegii individual definite pentru fiecare serviciu in parte. Privilegiile vor fi atribuite utilizatorilor individuali numai prin intermediul unor roluri adecvate. Un cont utilizator poate fi asociat cu un numar nelimitat de roluri structurate in mod ierarhic.

## 3. Nivelul Persistența informațiilor și a datelor

Informatia stocata, in baza de date relationala si utilizata in cadrul platformei trebuie sa prezinte urmatoarele caracteristici din punct de vedere al securitatii:

- Baza de date relationala va trebui sa permita restrictionarea accesului la nivelul obiectelor bazei de date;
- Baza de date trebuie sa permita aplicarea simultana a mai multor politici de securitate pe un acelasi obiect al bazei de date;
- Baza de date relationala trebuie sa ofere o lista cu operatiile pe care un grup sau o clasa de utilizatori le poate executa;
- Baza de date relationala trebuie sa ofere un mecanism de criptare a datelor;
- Baza de date relationala trebuie sa ofere un mecanism nativ de restrictionare a accesului utilizatorilor la nivel de inregistrare si coloana intr-o tabela.

## 4. Cerințe de securitate la nivelul platformei de virtualizare tip server

Sistemul informatic trebuie sa contina o solutie de gestiune integrata, unitara a utilizatorilor, la nivelul platformei de virtualizare si a sistemelor de operare virtualizate. Aceasta solutie trebuie sa:

- poata fi integrata cu platforma de virtualizare
- poata restrictiona accesul utilizatorilor in platforma de management al masinilor virtuale
- poata controla colectarea remote a logurilor
- poata controla administrarea remote a platformei de virtualizare
- poata descoperi si administra conturile privilegiate ale platformei de virtualizare
- poata descoperi masinile virtuale gazduite de platforma virtuala
- poata controla traficul de retea prin formarea de grupuri de securitate
- poata administra reguli de access la nivel de retea prin folosirea capabilitatilor native de firewall
- ofere un modul de management al parolelor conturilor privilegiate de pe platforma de virtualizare
- poata defini zone de securitate la nivelul retelei, astfel incat masinile dintr-o zona sa nu poata comunica decat cu masinile din aceeasi zona
- ofere o interfata unde utilizatorii pot da check-in / check-out unui cont privilegiat existent pe platforma de virtualizare; toate actiunile de checkin/checkout vor fi auditate cu data, ora, numele utilizatorului, contul care s-a accesat.
- ofere posibilitatea definirii de fluxuri de aprobari pentru aprobarea accesului unui utilizator la un cont de pe platforma de virtualizare.
- ofere posibilitatea colectarii, filtrarii si depozitarii evenimentelor generate de platforma de virtualizare
- ofere posibilitatea pastrarii evenimentelor colectate intr-o baza de date
- ofere posibilitatea arhivarii pe medii externe a evenimentelor mai vechi de o anumita perioada

### 5. Sistem de gestionare a dispozitivelor de criptare tip token USB

Solutia de securitate va implementa si un sistem de management al token-urilor care sa ofere o platforma de autentificare puternica, de tip multi-factor si care sa poata fi integrat cu urmatoarele sisteme:

- sisteme de control al accesului logic (autentificarea la statiile de lucru)
- un sistem de control al accesului la retea (autentificarea la anumite servicii de retea cum ar fi VPN)
- sisteme de tip LDAP pentru integrarea centralizata a utilizatorilor
- infrastructura cheii publice (PKI)

Sistemul de management al token-urilor trebuie sa aiba urmatoarele caracteristici:

- inrolarea utilizatorilor existenti dintr-un director LDAP
- crearea utilizatorilor direct in directorul LDAP
- capturarea fotografiei (pozei) utilizatorului si stocarea acesteia in directorul LDAP

- sa permita interfatarea cu solutii existente de inregistrare a utilizatorului (precum un sistem de management al identitatii printr-un API) si sa ofere metode pentru a administra in mod automat emiterea token-ului in timpul procesului de inregistrare
- crearea de profile personalizate pentru certificate folosite pentru: autentificare la statiile de lucru (logon), acces VPN, semnatura, s.a.
- emiterea smartcard-ului si a certificatelor
- activitati de administrare post emitere in mod centralizat (revocare certificate, eliberare token temporar, deblocare token blocat, incarcarea pe token de certificate aditionale, politici). Sistemul trebuie sa permita efectuarea acestor operatiuni cu tokenul in posesia utilizatorului, atunci cand acesta il conecteaza la statia de lucru (fara a fi necesar ca tokenurile sa fie transmise fizic administratorului sistemului care sa le proceseze pe fiecare in parte)
- Este obligatoriu ca sistemul sa permita utilizatorilor sa isi actualizeze cardurile in mod securizat, de la distanta, prin intermediul unei interfete web.Urmatoarele sarcini post-eliberare trebuie sa fie suportate de catre sistem:
    - Administrarea nu numai a credentialelor utilizatorului, dar si administrarea aplicatiilor stocate pe card (ex: appleturi)
    - Deblocarea cardului
    - Adaugarea, inlocuirea sau stergerea certificatelor digitale (ex: certificate expirate)
    - Adaugarea accesului securizat de la distanta pe baza unei parole valabile o singura data
    - Reciclarea cardului
    - Schimbarea PIN-ului
- Este obligatoriu ca sistemul sa ofere posibilitatea de self-service prin intermediul unei interfete Web. Utilizatorii trebuie sa poata realiza singuri urmatoarele operatii, prin intermediul unui browser, fara ajutorul unui operator aditional (dar, daca este necesar, cu validare din partea operatorului sau programarea dinainte a operatiunii):
    - Initializare si auto-personalizare electrica a tokenului pentru prima utilizare ( initializare cu un cod trimis utilizatorului prin email ca al doilea factor de autentificare)
    - Schimbarea PIN-ului
    - Deblocarea tokenului
    - Raportarea incidentelor privind tokenul (token pierdut/furat/ deteriorat/ uitat) si cererea unui token inlocuitor.
    - Actualizarea tokenului
- trebuie sa ofere urmatoarele functionalitati de tip help desk, (prin delegarea anumitor activitati catre un grup de utilizatori):

    - administrarea token-urilor: căutare, suspendare/rezumare, terminare, deblocare
    - administrarea cererilor: deblocare, inlocuire temporara/permanenta, actualizarea aplicatiei, re-eliberarea token-ului/cardului, reciclare, verificarea identitatii utilizatorului
    - deblocarea tokenului: Fata in fata, Asistat online, offline
    - administrarea aplicatiilor: suspendare/reactivare/revocare certificate
    - administrarea autentificarii utilizatorului in functie de intrebarile de securitate
- Este obligatoriu ca toate procedurile de tip self-service sa ofere proceduri aditionale de verificare si identificare a persoanei.
- Interfata de self-service trebuie sa ofere diferite metode de autentificare:
    - Parole LDAP
    - Cod de activare
    - Intrebari de securitate
    - Pe baza token-urilor
- Sistemul de management al token-urilor trebuie sa suporte:
    - Proces automat de reinnoire a certificatelor si raportarea printr-un email trimis operatorilor/administratorilor
    - Notificarea automata prin email trimis utilizatorului referitor la nevoia de actualizare a token-ului
    - Notificarea automata prin email trimis utilizatorului referitor la cereri de actualizare in asteptare pentru titularul dispozitivului.
- Interfata web administrativa a sistemului trebuie sa suporte autentificarea mutuala puternica a operatorilor, utilizand certificate digitale stocate pe token-uri.
- Este obligatoriu ca sistemul sa ofere cel putin doua metode alternative de autentificare care sa fie configurate pentru utilizatorii finali (detinatorii de token-uri), atunci cand este accesata interfata SCMS.
- Sistemul trebuie să suporte mecanisme duale de control pentru eliberarea și înlocuirea token-urilor, astfel încât să fie nevoie de un al doilea individ, diferit de cel care inițiază o cerere, pentru a aproba cererea inainte de a fi procesată.
- Sistemul trebuie să ofere mecanisme de securitate prin care doar organizația emitentă a token-urilor/smartcard-urilor să poată citi/scrie pe acestea – nici măcar producatorul token-urilor/smartcardurilor nu trebuie sa poata altera conținutul acestora fără a le deteriora iremediabil.
- Este obligatoriu ca orice comunicare dintre chipul token-ului și sistemul de management al acestora să fie cel puțin criptatăși semnată (sau sistemul de management trebuie să se conformeze standardului GlobalPlatform v.2.1.1 sau mai mare).
- Sistemul trebuie să permită auditarea  pentru toți operatorii și toate activitățile utilizatorilor

înregistrați în sistem.

- Sistemul trebuie să ofere un set de roluri predefinite ale operatorilor și de asemenea să permită definirea rolurilor pentru operatorii care se inregistreaza si care pot fi asociati numai cu grupuri particulare.
- trebuie sa ofere o interfata de tip web-based pentru toate operatiunile legate de management si de self-service ale utilizatorilor. Urmatoarele browsere trebuie suportate: Internet Explorer 6/7/8/9, Firefox 4, Mozilla etc
- Posibilitatea gestionarii atat de token-uri USB cat si smartcard-uri
- Sistemul trebuie sa suporte cel putin doua directoare LDAP comerciale majore:
    - obligatoriu: Microsoft Windows 2003/2008 Active Directory
    - obligatoriu una din urmatoarele: Microsoft ADAM sau Siemens DirX sau IBM Tivoli Directory Server sau Critical Path sau Novell eDir sau RedHat Directory sau altele.
- Sistemul trebuie sa suporte cel putin doua platforme comerciale RDBMS majore, precum MS SQL 2005, Oracle 10.
- Sa suporte configurarea pentru cazurile de load-balancing, failover si scalabilitate (sa suporte minim 10.000 de utilizatori si sa permita eliberarea a minim 500 de token-uri pe zi. )
- Trebuie sa fie capabil de a se interfata cu cel putin doua Autoritati de Certificare:
    - minim MS Microsoft CA 2003 / 2008
    - obligatoriu una din urmatoarele: VeriSign Managed PKI sau Entrust Authority Security Manager v7.1 SP3 sau CyberTrust Unicert cu ARM v5.3.5
- Solutia trebuie sa permita recuperarea cheilor de criptare
- Sa suporte token-uri cu memorie EEPROM de marime 64k, 80k, 128k (sau mai mult).
- Sa ofere support pentru minim urmatoarele sisteme de operare ale statiilor de lucru ale clientilor: Windows XP, Windows 2000, Windows 2003, Windows 2008 (32-, 64-bit), Vista (32-, 64-bit), Windows 7 (32-, 64-bit).
- SCMS trebuie sa fie in conformitate cu urmatoarele standarde:
    - JavaCard
    - GlobalPlatform 2.0.1 and 2.1.1
    - PC/SC
    - Certificate 1024- and 2048-bit RSA, X509
    - PKCS#7,#10,#11, Microsoft CAPI v2, SSLv3
    - Smart Card Interoperability Specifications GSC-IS v2.1
    - GSA Basic Services Interface (BSI)
    - LDAP v3
    - FIPS 201
- Este obligatoriu ca producatorul sistemului sa ofere cursuri de training si certificari pentru solutia de management al token-urilor, la intervale regulate, cu detaliile cursului disponibile.

### 1. Specificatii middleware pentru token-uri

- trebuie sa ofere suport serviciilor PKI pentru minim urmatoarele produse:
    - browser: Microsoft Internet Explorer 6 / 7 / 8, Firefox 1.5 / 2 / 3
    - logon: PKI-based cu smart card pentru minim: Windows 2000 / XP/ Vista / Win7 / 2003 / 2008;
    - client email pentru semnatura, cripate/decriptare: minim Microsoft Outlook 2000 / 2002 / 2003 / 2007, Thunderbird 1.5 - 16.0
- sa suporte tehnologia "java card" provenind de la cel putin 3 producatori.
- trebuie sa permita blocarea sau delogarea utilizatorului de la statia de lucru cand tokenul a fost indepartat.
- Este obligatoriu ca middleware-ul smart cardurilor sa ofere urmatoarele servicii utilizatorilor finali:
    - certificate digitale: vizualizare, importare, import/export rootCA, selectare/deselectare certificat pentru login
    - parole valabile o singura data (one-time-passwords): generarea in mod sincron si in mod challenge/response, resincronizare
    - ciclul de viata: initializare/schimbare PIN, deblocare token
    - iconita *system tray* care afiseaza activitatea token-ului
    - unealta de troubleshoot
    - diagnosticare avansata si urmarire
    - management central/de la distanta:
        - sistem de self-service pentru actualizarea securizata a token-urilor
    - verificarea automata a actualizarilor pentru token-uri si transmiterea unor mesaje asociate utilizatorilor

## 8. Cerinte privind subcomponenta de administrare a sistemului informatic

### 1. Administrare platforma hardware

Interfața de management centralizat:

- Sistemul trebuie să beneficieze de o interfață de management centralizat capabilă să administreze și să controleze toate resursele și mecanismele integrate:
    - blade-uri (mașini fizice)
    - interfețe I/O
- Sistemul trebuie să suporte adăugare și integrarea ulterioară a blade-urilor, toate putând fi controlate de la aceeași interfață de management
- Interfața de management trebuie să fie instalată pe o resursă hardware dedicată și complet

redundantă, alta decât blade-urile solicitate a fi instalate.
- Interfața trebuie să fie accesibilă cu o consolăși ca serviciu WEB pe porturi dedicate

## 2. Administrarea centralizata a server-elor fizice si virtuale

### 1. Cerinte ale interfetei de monitorizare si administrare:

- interfata unificata pentru sarcinii administrative (start, stop, reboot)
- o singura interfata de vizualizare a resurselor fizice si virtuale
- interfata de monitorizare sa fie bazata pe cel putin 3 componente:
    - vizualizarea evenimentelor – cum ar fi caderea unui echipament hardware, operatiuni de comutare automata a serverelor si rezultatul fiecarei operatiuni efectuate;
    - operatiuni recente – afisarea progresul diferitelor operatiuni efectuate;
    - monitorizarea retelei – posibilitatea de a vizualiza si corela retelele virtuale si fizice, prin intermediul hartii integrate;
- sa permita integrarea cu un soft de management extern, pentru detectarea cu precizie a partilor defectuoase din cadrul resurselor administrate;
- sa poata furniza date despre consumul de energie, iar acestea sa poata fi afisate in forma unui grafic sau sa poata fi exportate intr-un format csv, pentru o analiza ulterioara;
- monitorizare centralizata mixta pentru servere fizice si virtuale;

### 2. Functionalitati minimale:

- sa functioneze in medii multi-hypervisor;
- sa suporte migrarea in timp real pentru platformele hypervisor x86: VMware vSphere, Microsoft Hyper-V, Citrix XenServer, KVM, Oracle VM etc
- sa suporte setarea automata de resurse multiple intr-o operatiune de grup importand un fisier, in format csv, de definire a sistemului, care sa contina toate setarile si informatiile privind configuratia;
- sa permita operatiuni de migrare in timp real a serverelor virtuale, declansate in mod uniform pentru toate produsele hypervisor suportate, direct din consola de administrare si care sa se realizeze fara timp de nefunctionare si cu suport pentru echilibrarea dinamica a incarcarii;
- sa pastreze pozitia initiala a fiecarui client al masinii virtuale și să permita migrarea inapoi in orice moment in locatia lor originala;
- sa inglobeze funcționalitatea de a comuta complet gazdele masinii virtuale, incluzand toate elementele in functiune ale masinii virtuale , catre un server de rezerva;
- comutarea sa poata fi initializata manual sau automat prin funtia deauto-recuperare;
- sa suporte back-up si restaurare completa a imaginii boot disk-ului incluzand sistemul de operare si alte date stocate pe acel disk;
- sa ofere o functie integrata de clonare a serverului care sa permita distributia unei imagini clonate, catre unul sau mai multe servere fizice;
- imaginile sa fie gestionate centralizat si stocate de catre serverele de admiistrare;
- auto-recuperarea serverelor cazute, fara interventia operatorului;
- sa ofere o disponibilitate crescuta prin folosirea unor servere de rezerva cu sisteme fizice si servere cu gazde virtuale;
- sa suporte virtualizare I/O pe servere, fara sa tina cont de tipul acestora (rack, tower si blade)
- sa foloseasca tehnologia SAN-boot in combinatie cu tehnologia de virtualizare I/O pentru o disponibilitate crescuta;

- sa inglobeze functia de Virtualizare a I/O permitind administartorului sa adauge, sa mentina sau sa elimine servere fara sa afecteze setarile retelei si fara sa fi nevoie de re-cablare;
- sa aiba functia de "HBA Address Rename Service" sau echivalent;
- sa suporte boot-area serverelor din sistemul de stocare al retelei atasate via Fibre Channel cat si boot-area serverelor de pe un disk local;
- sa permita configurarea retelelor fizice si virtual;
- modul de diagnoza a conexiunilor de retea, intre toate resursele administrate;

## 3. Cerințe privind soluția de monitorizare a performantelor platformei portal si a solutiei de gestiune a tichetelor

In vederea monitorizarii platfomei este necesara o solutie care sa asigure urmarirea parametrilor de functioanare a acesteia, experienta realtime a utilizatorilor, pentru a da posibilitatea de interventie proactiva si reactiva de remediere a eventualelor probleme.

Solutia propusa trebuie sa respecte urmatoarele cerinte tehnico-functionale:

- Solutia trebuie sa permita urmarirea traficului real (de productie) http sau https din retea generat de platforma fara a opera modificari asupra acestuia.
- Solutia trebuie sa permita de asemenea si instrumentarea la nivel de cod a claselor Java sau .Net in vederea analizei performantei platformei la acest nivel.
- Solutia trebuie sa ofere posibilitatea de a prelua statisticile din logurile serverelor (web server, database server, application server)
- Solutia trebuie sa ofere posibilitatea de a crea agenti care sa preia informatii si statistici din loguri "non-standard".
- Monitorizarea sa aiba loc 24x7x365 atat pentru traficul web cat si pentru aplicatie.
- Incarcarea suplimentara de consum de resurse prin instrumentare sa nu fie mai mare de 3%.
- Sa aiba capabilitatea de a detecta MemoryLeak-uri direct pe aplicatia de productie.
- Sa aiba capabilitatea de a detecta schimbarile survenite pe fisierele de configurare ale aplicatiei si sa realizeze corelarea cu problemele detectate
- Sa aiba capabilitatea de a genera tranzactii sintetice (gen robot) simuland actiunile unui utilizator, avand posibilitatea de a diferentia traficul simulat de traficul real.
- Sa aiba capabilitatea de a monitoriza servicii web
- Sa aiba capabilitatea de a detecta in mod automat dependintele intre componentele unei arhitecturi de tip SOA si tranzactiile business monitorizate. Sa aiba capabilitatea de a afisa in mod grafic (harta) aceste dependinte.
- Sa monitorizeze real-time JVM-ul sau CLI-ul din punct de vedere: utilizare memorie, cache, conexiuni la baza de date.
- Sa monitorizeze real-time thread-urile de conexiune blocate catre baza de date.
- Sa monitorizeze toate apelurile SQL si sa raporteze pe cele cu performanta sub anumite praguri definite.
- Aplicatia trebuie sa prezinte statistici despre toate frazele SQL trimise catre serverul de baze de date
- Aplicatia trebuie sa ofere urmatoarele statistici pentru frazele sql, metode, clase si url-uri aflate in monitorizare:
    - timpii de raspuns minim, maxim si mediu
    - numarul de apelari si raspunsuri concurente
    - numarul de erori si detalii despre aceste erori

    - numarul de metode, url-uri si fraze SQL ramase agatate (timpul de executie mai mare de 30 de secunde).
- In cazul aparitiei unei probleme, pentru tranzactia care a generat problema aplicatia trebuie sa ofere statistici complete incepand cu faza initiala (click utilizator) pana la apelul catre baza de date
- Colectarea, procesarea si afisarea in timp real a experientei utilizatorilor (frontend) in stransa legatura cu aplicatiile/interfetele pe care acestia le folosesc (backend); sa aiba posibilitate de a corela raspunsurile URL cu componentele aplicatiei implicate de aceste apeluri.
- Trasabilitatea actiunilor utilizatorilor, de la cererea initiala facuta in aplicatie (de exemplu un simplu click pe un buton) – pana la toate raspunsurile primate din aplicatie sau de la sistemele conexe.
- Posibilitatea de a identifica o tranzactie web prin utilizator, locatie sau alt parametru definit.
- Posibilitatea de a grupa tranzactiile web in servicii business si monitorizarea la nivel de serviciu business.
- Rapoarte si KPI-uri  pentru validarea performantelor aplicatiei monitorizate
- Posibilitatea de a identifica in timp real problemele pe care utilizatorii le au in lucrul cu interfata sau cu aplicatiile monitorizate
- Capabilitati de inregistrare si redare a intregii sesiuni a unui utilizator de la momentul in care a inceput sa lucreze cu interfata/aplicatia pana la momentul in care a intampinat o problema.
- Monitorizare  in timp real cu functionalitati ca:
    - Tablouri de bord
    - Diagnostice ale sesiunilor utilziatorilor
    - Inregistrare/Redare a unei intregi sesiuni
    - Trasabilitate a unei tranzactii de business
- Administrare si monitorizare la nivel de serviciu:
    - Praguri de servicii cu alertare in cazul depasirii acestora
- Posibilitatea de a defini SLA-uri bazate pe metrice de performanta a aplicatiei si posibilitatea de alertare in cazul depasirii acestora.
- Solutia trebuie sa identifice si sa prioritizeze problemele care ar afecta calitatea serviciilor catre utilizatorul final prin analizarea in timp real a tranzactiilor individuale pentru fiecare utilizator;
- Rapoarte  analitice de utilizare a sitemelor monitorizate cu urmatoarele  functionalitati:
    - Tablouri de bord customizabile la nivel de grup de utilizatori/aplicatii
    - Analize ale KPI-urilor
    - Analize detaliate de tip drill down
    - Analize ale tranzactiilor abandonate sau nefinalizate cu succes
- Sa pastreze datele statistice si metricele pe o perioda de retentie definita. Sa poata arhiva aceste date dupa o perioda.
- Sa mentina un istoric cu toate evenimentele de securitate care au aparut in utilizarea solutiei.
- Posibilitatea de monitoriza metrice de performanta pentru servere de aplicatie ca portaluri: Websphere, SharePoint, etc..
- Posibilitatea de a functiona intr-un mediu virtualizat (toate componentele).
- Ofertantul trebuie sa ofere implementarea solutiei de monitorizare a performantei. In vederea acestui lucru,  ofertantul va dovedi capacitatea de implementarea prin includerea in echipa de implementare a doua persoane cu certificari de implementare nivel maxim de la producatorul solutiei.

## 4. Cerințe privind subcomponenta de salvare si recuperarea datelor

Soluția de salvare și restaurare a datelor trebuie să aibă o structură de management centralizat și să ofere protecție pentru platforma de portal, pentru componenta colaborativa tip CRM (gestiunea tichetelor) si pentru platforma de virtualizare desktop

Oferta va include în preț servicii de consultanță tehnică prin specialişti ai Ofertantului şi specialişti ai producătorului. Se solicită ca implicarea specialiştilor certificațide producătorsă fie în toate etapele de derulare după cum urmează:

- Analiză;
- Elaborare arhitectură soluție;
- Implementare și configurare;
- Testare și stabilizare;
- Elaborare documentație și transfer de cunoștințe către persoanele desemnate din partea beneficiarului.

### 1. Cerințe generale pentru Soluția de salvare si recuperare a datelor:

- Optimizarea timpului de răspuns al echipei IT în rezolvarea incidentelor
- Automatizarea activităților de backup și restore IT și eliminarea sarcinilor repetitive, mari consumatoare de timp, ale echipei IT;
- Simplificarea cazurilor de restore prin delegarea drepturilor administrative.

### 2. Cerințe minime obligatorii

Soluție de backup și restaurare în caz de dezastru pentru infrastructura IT trebuie să permită operațiuni și facilități precum:

- Soluția de back-up trebuie să asigure o protecțe eficientă a datelor împotriva erorilor și a dezastrelor prin stocarea copiilor de salvare și arhivare pe medii de stocare “online” și, dacă este cazul, “offline”;
- Soluția de backup trebuie să conțină și componenta de backup și restaurare date pentru subsistemele de baze de date și colaborare fără încărcare suplimentară la nivelul serverelor de producție;
- Să asigure un back-up centralizat prin consola grafică definită la nivelul centrului de date de producție central;
- Aplicația de backup asigură instalarea și upgrade-ul simplu al agenților de backup direct din consola centrală de administrare prin utilizarea serverului cu rol de instalare și upgrade agenți backup;
- Aplicația trebuie să permită efectuarea back-up-ului doar pentru fișierele care au suferit schimbări de la ultimul back-up și pentru fișierele nou create;
- Operare complet automată a mediilor de stocare în sesiunile de backup;
- Aplicația trebuie să genereze rapoarte locale, cât și rapoarte consolidate asupra întregului mediu de back-up, cât și a operațiunilor de back-up;
- Posibilitatea de a efectua back-up la nivel de date, server, sistem de operare atât pentru mediul fizic, cât și virtual la un interval minim de 15 minute, fără întreruperea accesului utilizatorilor la acestea;

- Soluția va permite protejarea mașinilor virtuale, fără a încetini sau întrerupe funcționalitatea acestora;
- Posibilitatea de a efectua ușor restaurarea datelor în caz de dezastru;
- Posibilitatea de a oferi utilizatorilor drepturi de restaurare a datelor;
- Soluția trebuie să ofere suport pentru mediile virtuale componente ale sistemului;
- Posibilitatea delegării drepturilor administrative și de restore;
- Posibilitatea de a efectua back-up pentru minim Exchange Server 2007 si Exchange 2010 Server;
- Posibilitatea de a efectua back-up pentru minim Office Sharepoint 2007 si 2010 Server;
- Posibilitatea de a efectua back-up pentru baze de date;
- Restaurarea serverelor dintr-o singura operație – bare metal restore, fără a fi necesara reinstalarea sistemului de operare, aplicației și datelor succesiv;
- Posibilitatea de a avea arhitecturi de backup redundante prin folosirea unor servere în locațiile de disaster recovery care să ofere backup pentru serverul de backup din locația primară;
- Soluția trebuie să permită restaurarea unei baze de date într-o locație alternativă pe același server fără a perturba utilizatorii bazei de date în lucru;
- Soluția trebuie să permită restaurarea bazei de date pe un alt server;
- Soluția trebuie să permită restaurarea unei baze de date pe bandă;
- Soluția trebuie să ofere protecție pentru serverele existente in sediul autoritatii contractante de tip stand-alone Microsoft Exchange 2007 și 2010;
- Soluția trebuie să ofere protecție pentru clustere-le existente in sediul autoritatii contractante de tip Exchange Server 2007 de tip MSCS, CCR și LCR;
- Soluția trebuie să ofere protecție pentru clustere Exchange Server 2010 de tip DAG;
- Trebuie să ofere posibilitatea de restaurare la nivel de:
    - Storage group;
    - DataBase;
    - Mailbox;
- Restaurarea de la ultimul back-up să se poată efectua în locația originală;
- În momentul efectuării operației de back-up, soluția trebuie să ofere protecție pentru toate serverele din fermă și să efectueze backup al datelor de pe toate serverele componente;
- Neefectuarea unui backup pentru o singură bază de date să nu implice neefectuarea backup-ului pentru întreaga fermă;
- Posibilitatea de a restaura la nivel de obiect, bază de date, fermă.

## 9. Cerințe privind echipamente de calcul şi echipamentele periferice

Toate echipamentele furnizate în cadrul acestui proiect trebuie să fie noi .

### 1. Echipamente server pentru virtulizare DataCenter

Pentru procesare solutia prevede echipamente de tip lamelar (blade servers), pe arhitectura x86_64, sau similara. Fiecare din aceste echipamente va avea urmatoarea configuratie minima obligatorie:

#### 1. Cerințe Șasiu:

Serverele blade trebuie sa fie acomodate intr-un șasiu rack-abil, cu urmatoarele caracteristici minimale:

- Dimensiuni maxima: 10 U
- Sistemul trebuie sa suporte minim 16 blade-uri cu cate 2 procesoare CISC, pentru a asigura un minim de 28 core/unitate rack.
- Sursele de curent trebuie sa fie in numar de minim 4 (eficienta minim 90%) cu redundanta (capabile sa asigure functionarea sasiului chiar si in eventualitatea defectarii a oricare trei surse).
- Implementarea fizică a conexiunilor trebuie realizata printr-un back-plane de mare viteza- minim 8,960 Gb/s latime de bandași latență redusă, care să asigure minim patru canale de comunicație redundante per blade.
- Tehnologia utilizata pentru conectivitate trebuie sa permita gruparea logica a oricaror doua sau mai multe porturi Ethernet / Fiber Channel, corespunzand oricarui slot pentru servere blade din sasiu, intr-un singur port extern ale carui caracteristici (MAC, WWN) nu se vor schimba atunci cand un server blade este inlocuit.
- Panou LCD pentru monitorizarea si management
- Memorie minim suportata de 13000 GB RAM
- Capacitate interna de stocare de minim 50 TB
- Interfetele I/O trebuie sa fie consolidate cu ajutorul a minim 4 switch blade-uri (pentru redundanta) intr-un numar de porturi externe dupa cum urmeaza:
    - Minim 36 porturi Gigabit Ethernet impartite pe 2 switch-uri pentru asigurarea redundantei tuturor conexiunilor LAN
    - Minim 2 porturi Fiber Channel impartite pe 2 switch-uri pentru asigurarea redundantei tuturor conexiunilor SAN, pentru fiecare server blade
    - 2 porturi seriale redundante si 4 porturi Ethernet redundante dedicate pentru management.
- Arhitectura sistemului trebuie sa permita implementarea unor solutii de Load Balancing si FailOver pentru porturile de Ethernet si Fiber Channel
- Sasiul trebuie sa poate acomoda cel putin 4 switch blade de tip Ethernet si 4 switch blade de tip Fiber Channel necesare in cazul scalarii ulterioare a intregii solutii.

## 2. Cerințe server lamelar

| | |
|---|---|
| Procesor | 2 procesoare instalate tip Eight Core Intel Xeon 2.3 GHz (12MB Third Level Cache ECC) 8 GT, bus QPI, , sau echivalent |
| Memorie cache (TLC) | Minim 20 MB |
| Memorie RAM | 64 GB DDR3 1333, PC3-10600 SDDC instalata;<br>Suport pentru protectie de tip memorie in oglinda (memory mirroring)<br>Suport pentru protectie memorie de tip rezerva calda (hot spare memory)<br>12 slot-uri DIMM pentru o capacitate maxima in interiorul blade-ului de minim 384Gb |

| | |
|---|---|
| Placa retea | Integrata, minimum 2 porturi 10 Gbit/s Ethernet, suport pentru Intel® VT-c (inclusiv I/OAT, VMDq, sau tehnologii echivalente ) |
| Placa fibra optica | Minimum 2 porturi x 8Gb/s |
| Porturi | 1 x VGA, 5 x USB, 1 x serial (accesibile frontal) |
| Sloturi | 2 x slot-uri pentru expansiune (conectivitate dupa standardul PCI-Express Gen3 x8) |
| Hard disk | Fara hard-diskuri interne, să conțină modul flash pentru hipervizorul solutiei de virtualizare |
| Placa video | Integrata, minim 32Mb memorie video |
| Management | Aplicatie de management operational dezvoltata de producatorul sistemului de calcul, cu urmatoarele functii: monitorizarea starii sistemului, managementul evenimentelor si alarmelor, inventarul componentelor, inventarul si instalarea up-date-urilor si patch-urilor, analiza performantei, diagnoza on-line, restartarea si reconfigurarea automata a serverului, analiza si previzionarea defectarii componentelor (PFA)<br>Chipset pentru remote management integrat compatibil IPMI 2.0 cu acces prin web browser cu securizare prin criptare SSL 128 bit |
| Compatibilitate cu sisteme de operare | Microsoft® Microsoft® Hyper-V™ Server 2008 R2<br>Microsoft® Windows Server® 2008 R2 Datacenter, Enterprise, Standard<br>Microsoft® Windows HPC Server® 2008 R2 Suite<br>Microsoft® Windows® Small Business Server Standard 2011<br>Microsoft® Windows® Server 2008 Datacenter, Enterprise,Standard<br>Microsoft® Windows Server® 2003 Enterprise Edition<br>Microsoft® Windows Server® 2003 Standard Edition<br>VMware vSphere™<br>Novell® SUSE Linux Enterprise Server 11, 10, 10 with XEN<br>Red Hat® Enterprise Linux 6, 5, 5 with XEN |

## 2. Echipament server pentru virtualizarea infrastructurii desktop

Aritectura ce va asigura suportul pentru soluția de virtualizare desktop trebuie să satisfacă următoarele cerințe minime obligatorii:

| **Componenta** | **Cerința tehnică minimală** |
|---|---|
| Placa de baza | Fabricata sub aceeasi marca cu sistemul de calcul |
| Chipset placa de baza | Intel® C600 sau echivalent |
| Procesor instalat | 2 x Intel Xeon Eight Core, 2 GHz sau echivalent |
| Memorie cache level III (TLC) | Minim 20 MB |
| Magistrala de memorie RAM | 1600 MHz |
| Suport memorie RAM | Minim 24 DIMM-uri, suport pentru 768GB RAM |
| Metode de protectie a memoriei suportate: | Advanced ECC<br>SDDC (Chipkill™)<br>Hot-spare memory<br>Memory mirroring |
| Memorie instalata | 96 GB DDR3 1600 MHz PC3-12800 registered ECC |
| Controller hard-discuri | SAS 6G RAID controller pe magistrala PCIe 4x pentru conectarea hard-discurilor interne SAS, SATA sau SSD cu suport pentru RAID 0, 1 |
| Suport hard-discuri | Minim 8 sloturi SFF (2,5”) pentru hard-discuri hotplug SAS sau SATA |
| Hard-discuri instalate | Fara hard-diskuri instalate, sa conțină modul flash pentru hipervizorul solutiei de virtualizare |
| Unitate optică | Unitate optica tip DVD-RW integrata in carcasa |
| Interfața grafica | Integrată |

| | |
|---|---|
| Interfata de rețea (on-board) | 2 x Ethernet 10/100/1000 Mbps RJ 45, accelerare I/O, iSCSI boot<br><br>2 x Ethernet 10 Gbps RJ 45, accelerare I/O, iSCSI boot<br><br>1 x Ethernet 10/100 RJ45 dedicat remote management |
| Sloturi de expansiune | Minim 5 sloturi PCI-Express Gen3 x8 si 2 sloturi PCI-Express Gen3 x16 |
| Conectori interfete intrare/iesire | 1 x serial, 1 x monitor, min 8 x USB (dintre care minim 2 interne) |
| Carcasa | Rack-abila, maxim 2U, cu ventilatoare hot-plug redundante |
| Sursa de alimentare | Eficienta minnim 92%, doua surse pentru redundanta |
| Consum energetic | Putere activa: maxim 800W |
| Sistem de operare | Compatibil cu sistemul hardware ofertat |
| Compatibilitate cu sisteme de operare | Microsoft® Microsoft® Hyper-V™ Server 2008 R2<br>Microsoft® Windows Server® 2008 R2 Datacenter, Enterprise, Standard<br>Microsoft® Windows HPC Server® 2008 R2 Suite<br>Microsoft® Windows® Small Business Server Standard 2011<br>Microsoft® Windows® Server 2008 Datacenter, Enterprise,Standard<br>Microsoft® Windows Server® 2003 Enterprise Edition<br>Microsoft® Windows Server® 2003 Standard Edition<br>VMware vSphere™<br>Novell® SUSE Linux Enterprise Server 11, 10, 10 with XEN<br>Red Hat® Enterprise Linux 6, 5, 5 with XEN |
| Management | -aplicatie pentru instalarea si configurarea serverului dezvoltata de producatorul serverului capabila de instalare locala si remote in mod neasistat, inclusiv configurare RAID;<br><br>-aplicatie de management operational cu urmatoarele functii: monitorizarea starii sistemului, managementul evenimentelor si alarmelor, inventarul componentelor, inventarul si instalarea up-date-urilor si patch-urilor, analiza performantei, diagnoza on-line, restartarea si reconfigurarea automata a serverului, analiza si |

previzionarea defectarii componentelor (PFA);

-chipset pentru remote management integrat compatibil IPMI 2.0 cu acces prin web browser cu securizare prin criptare SSL 128 bit, integrat cu aplicatia de management, redirectarea interfetei video

| | |
|---|---|
| Conformitate cu standarde europeene | Certificare CE conform directivelor UE: |
| | - Product safety: IEC 60950-1 / EN 609501- |
| | - Electro magnetic compatibility: EN 55 022 class A, EN 55024, EN 61000-3-2 / 3-3 |
| | - Declaration of conformity: 89/336/EEC(EMV); 73/23 EEC(LVD) |
| Conformitate cu standardele privind managementul calitatii | ISO 9001, |

### 3. Echipament server pentru infrastructura de telefonie tip 1

Cerinte hardware obligatorii pentru echipamentul server de comunicatii:

| | |
|---|---|
| Tip carcasă | Server base unit 2,5" cu doua surse redundante, rack mountable |
| Procesoare instalate | 2 * Intel® Xeon® Processor E5-2420 (6 Core, 1.90GHz, 15MB) sau echivalent |
| Memoria instalată | 4 * 8GB (1x 8GB) DDR3L-1600, Registered |
| Protecția dicurilor interne / controller | 1 * RAID Controller (512 MB, RAID 0/1/5/6) (PCIe2 X8)<br>1 * Battery Back-up Unit (BBU) |
| Discuri instalate | 3 * HDD SAS 2.5" HotSwap 15K (6Gbps) 300GB |
| Unitate optică | 1 * Internal Slim DVD Drive |
| alimentare | 2 * Hot swap si Redundant 450w 80+ Platinium power supply |
| Consolă de administrare | 1 * Remote KVM si Media License Key Pilot3 |
| Cerințe I/O | 5 * Sloturi de extindere disponibile |

| | |
|---|---|
| Cerințe interfețe rețea | 2x1000 BASE-T/100 BASE-TX/10 BASE-T instalate<br>1x100BASE-TX pentru Management instalat |
| Cerința de consum de energie | Consum maxim: 815 VA/ 800W pentru ambele surse |
| Dimensiuni | Dimensiuni maxime: 450 mm x 725 mm x 90 mm<br>Greutate maxima: 35 kg |
| Sistem de operare instalat | sistem de operare licențiat pentru tipul de echipament ofertat |

## 4. Echipament server pentru infrastructura de telefonie tip 2

| | |
|---|---|
| Tip carcasă | Server base unit 2,5" cu doua surse redundante, rack mountable |
| Surse de Alimentare | Redundante, Hot swap consum maxim 750w 80+ gold power supply |
| Procesoare instalate | 2 * Intel® Xeon® Processor E5645 (6 Core, 2.40GHz, 12MB, 5.86GT/s) sau echivalent |
| Memorie instalată | 8 * 4GB DDR3-1333, 1.35V/1.5V, Registered (1x 4GB, PC3-10600) |
| Cerințe I/O disponibile | 4 x PCI EXPRESS 2.0<br>1x PCI EXPRESS(x4) dedicat pentru conectarea la baa de date |
| Protecția dicurilor interne / controller | 1 * LSI MegaRAID Sas/Sata 9264-8i controller, RAID0/1/5/6, 256MB, BBU less, Int. X8<br>1 * Battery Backup Unit for LSI MegaRAID SAS8708EM2 and 9264-8i controllers |
| Discuri instalate | 4 * HDD SAS 2.5" HotSwap 15K (6Gbps) 146.5GB |
| Interfete de retea instalate | 2 * Intel PRO/1000 PT Dual Port Gigabit Copper NIC (2x 10/100/1000, 2x RJ45, PCI Express X4, ALB/AFT)<br>1x100BASE-TX pentru Management |
| Unitate optică | 1 * SATA DVD superMulti Slim 4,7/9,4GB |
| Dimensiuni fizice | Dimensiuni maxime: 450 mm x 725 mm x 90 mm |
| Greutate | Greutate maxima: 35 kg |

## 5. Echipament extern pentru stocarea datelor

### 1. Cerințe subsistem de stocare pe disc

1. Sistem de stocare centralizata cu minim 2 controllere redundante si hot-plug, cu failover automat, sistemul va fi tolerant la defectarea unui controler, asigurând integritatea şi disponibilitatea datelor în mod transparent pentru aplicații.
2. Sistemul va fi livrat cu urmatoarele caracteristici hardware :

- Memorie cache: minim 12 GB

- Capacitate de stocare instalata: minim 24 HDD 600GB SAS. Redundanța la nivelul unităților de disc va fi asigurată printr-o tehnologie RAID.

- Numar de porturi I/O : minim 4 FC 8Gbps , minim 8 Ethernet 1 Gbps . Suport pentru porturi I/O iSCSI 10Gbps .

- Controllere, surse de alimentare si sisteme de ventilatie redundante si hot-swappable

- Scalabilitate de minim 500 HDD prin upgrade cu sertare de discuri, sau prin inlocuirea controllerelor fara a migra datele si discurile existente.

3. Sistemul trebuie sa includa serviciu de acces la date simultan şi concurent în mod multiprotocol, la nivel de bloc şi la nivel de fişier, de pe acelaşi nod de control pentru : FC, iSCSI , CIFS , NFS.
4. Sistemul trebuie sa ofere suport pentru :

- definirea de volume de tip WORM (Write Once Read Many)

- backup si restaurare disk-to-disk, bi-directional, impreuna cu alte sisteme din aceeasi familie de produs

- realizarea de copii la distanta a seturilor de date in maniera sincrona si asincrona si integrarea cel putin a următoarelor tehnologii pentru optimizarea replicarii de date : deduplicarea datelor, compresia datelor, replicarea incrementala la nivelul blocurilor de date noi.

5. Furnizorul va include toate subansamblele, accesoriile si licentele software necesare interconectarii sistemului de stocare SAN in structura sistemului informatic precum si serviciile de instalare si configurare conform specificatiilor producatorului echipamentului.
6. Echipamentul va fi livrat cu 3 ani suport software si hardware cu timp de livrare pentru piese de schimb : urmatoarea zi lucratoare.

### 2. Cerințe subistem de stocare pe banda

1. Sistem de stocare pe banda cu suport pentru o capacitate de minim 37 TB nativ, fără compresie.
2. Sistemul trebuie sa fie echipat cu minim 1 x LTO-5 drive , interfață FC , 8Gbps. Sistemul trebuie sa aiba activate minim 12 sloturi de banda.
3. Sistemul trebuie ofere suport pentru drive de banda cu interfata SAS 2.0 6Gbps cat si pt drive de banda cu interfata FC 8Gbps , LTO-4 si LTO-5. Sistemul trebuie sa detina suport pentru minim doua drive-uri de banda .
4. Suport pentru criptarea datelor , suport pentru partitionare in minim doua biblioteci logice, design flexibil - minim doua magazii pentru benzi .
5. Casete de benzi : sistemul se va livra cu 12 casete de benzi LTO-5 , sistemul trebuie sa ofere suport pentru casete tip WORM, sistemul trebuie sa suporte mail slot pentru minim 3 casete.

6. Management: GUI, remote management, port Ethernet pt upgrade de firmware, panou LCD .
7. Sistemul trebuie sa includa un mecanism robotizat autoloader cu cititor de coduri de bare
8. Sistemul trebuie sa includa toate accesoriile necesare conectarii in SAN si alimentarii cu energie electrica, Rack Kit, 1x caseta de curatare, 1 x cablu Ethernet. Sistemul cu benzi trebuie sa aiba o dimensiune de maxim 2 unitati de rack.

## 6. Echipament Cabinet cu UPS-uri

Echipamentele hardware vor fi integrate intr-un ansamblu cabinet tip RACK, echipat cu switch, consola tip KVM si surse neintreruptibile de tensiune, cu urmatoarele specificatii tehnice:

| **Denumire** | **Echipament Cabinet modular de tip RACK** |
|---|---|
| Înălțime utilă | • Capacitate utilă de minim 42 unitati rack; |
| Uși și panouri laterale | • Uși și panouri laterale demontabile;<br>• Posibilitatea de schimbare a sensului de deschidere a usi fata;<br>• Posibilitatea de a securiza la nivel fizic echipamentele aflate in interior folosind incuietori cu chei special pentru ușile față-spate și panourile laterale;<br>• Să ofere acces facil pentru instalara/dezinstalarea echipamentelor prin inlaturarea temporara a usilor;<br>• 0 distanta de max. 70 cm pentru deschiderea usilor fata/spate;<br>• Rack-ul va fi prevazut cu intrari/iesiri pentru cabluri electrice ,date,RF prin locasuri special concepute in acest scop; |
| Ventilare | • Ventilare libera cu usi fata-spate perforate in proportie de minim 80 %;<br>• Unitatile rack vor fi acoperite cu panouri false , pentru a garanta ventilare cat mai buna; |
| Compatibilitate | • Echipamentul cabinet sa fie produs de acelasi furnizor ca si echipamentul de tip sasiu server lamelar in ideea de a se asigura o compatibilitate optima intre dispozitive |
| Incarcare | • Sa suporte o incarcare de minim 1000 Kg; |
| **Denumire** | **Sursa neintreruptibila de tensiune tip UPS** |
| Iesire | • Structura de alimentare de tip UPS de tip on-line dubla conversie, monofazata (1/1) ;<br>• Capacitatea de putere : de minim 10KVA ;<br>• Voltaj nominal iesire : 230V ;<br>• Distorsiuni Voltaj nominal : max. 3% ;<br>• Frecventa de iesire : 50 – 60 Hz (+/- 3 Hz);<br>• Forma de unda : sinusoidala ; |

| | |
|---|---|
| | • Conectori iesire : 4 x IEC 320 C13, 4 x IEC 320 C19, 4 x IEC jumpers ; |
| Intrare | • Voltaj nominal de intrare : 230V ;<br>• Frecventa de intrare : 50 – 60 Hz (+/- 5Hz detectie automata) ;<br>• Gama tensiunilor de intrare : 160 – 280V ; |
| Baterii si timp de functionare | • Componentele interne active ale unitatii UPS, inclusiv bateriile, vor fi de tip hot-swap si vor permite deservirea (inclusiv inlocuirea acestora) fara oprirea sarcinii ;<br>• Eficienta la incarcare maxima : min. 92% ;<br>• Autonomia UPS-ului : min. 50 minute la o incarcare de 75% ; |
| Protectie | • Unitatea UPS va fi echipata cu functie interna activa de comutare neasistata, automata si transparenta pe bypass fara oprirea sarcinii atunci cand componentele interne de conversie si corectie ale unitatii nu fac fata sau prezinta erori de functionare ; |
| Management | • Interfata tip DB-9 RS-232<br>• Panou de control tip LED cu funtie de avertizare vizuala pentru urmatoarele stari ale echipamentului: functional, functionare pe baterie, indicator de inlocuire a bateriilor, supraicarcare si indicator pentru modul bypass;<br>• Alarma sonora: cu moduri distincete de atentionare pentru trecerea in modul de functionare pe bateriisi baterie scazuta;<br>• Unitatea UPS va fi echipata cu modul intern amovibil de management in retea (SNMP sau asimilat) ; |
| Mediu functionare | • Temperatura: 0 – 40 C;<br>• Umiditate: 0 – 95%;<br>• Zgomot: 55 db;<br>• Caldura disipat: max. 2300 BTU/h |
| Dimensiune | • Montabil in Rack de 19 ‘’ , inaltime de maxim 6 RU ; |
| **Denumire** | **Componeta distributie tip PDU** |
| Conectori | • Pentru alimentarea echipamentelor se vor folosi unitati de tip Server PDU, cu urmatorii conectori : 6 x 16A si 4x10A IEC320 ;<br>• Nu este acceptabila cascadarea pe mai mult de doua niveluri de distributie, inclusiv unitatea UPS PDU. |
| Dimensiuni | • Echipamentul va ocupa max. 2 RU ; |
| **Denumire** | **Consola locala tip KVM** |

| | |
|---|---|
| Monitor | • Minim 17 inch;<br>• Suport pentru afisare de rezolutii native de (min.) 1280x1024 ;<br>• Contrast 450 :1 (TYP) ;<br>• Luminozitate 200cd/m2 |
| Tastatura | • Tastatura standard cu minim 87 taste si touchpad cu 2 butoane si functie de scrolling; |
| Dimensiuni | • Montabil in rack 19 inch , kit pentru montare inclus ;<br>• Dimensiuni maxim admise, fara kit-ul de montare in rack (W x D x H) : 500mm x 450mm x 50 mm ;<br>• Greutate maxim admisa : 15kg (kit-ul de montare in rack inclus) ;<br>• Consola va ocupa, pliata, un spatiu optim de 1U in rack ; |
| Mediu de functionare | • Umiditate de operare : 10-85% (fara condensare) ;<br>• Consum : max. 30W ; |

| | |
|---|---|
| **Denumire** | **Switch KVM** |
| Porturi | • Echipamentul va fi prevazut cu 16 porturi pentru conectarea la servere;<br>• Conectica necesara echiparii celor 16 porturi va fi inclusa in oferta;<br>• Monitoare suportate: VGA, SVGA, XGA, XGA-II;<br>• Tastaturi suportate: USB, RC23/24, RC24/RC25; |
| Rezolutie | • Rezolutie video suportata: 1280 x 1024; |
| Dimensiuni | • Echipament montabil in rack (max. 1U), kit de montare inclus;<br>• Dimensiuni maxime admise (WxDxH): 450mm x 280mm x 50mm<br>• Sa poata fi colocat imptreuna cu **Consola locala tip KVM in acelasi unitate de rack** |
| Mediu de functionare | • Consum: max. 16W |

## 7. Echipamente rețelistică

### Router

| | |
|---|---|
| Cerinte tehnice generale | - Sasiu modular, montabil in rack de 19”;<br>- Toate componente sistemului trebuie sa fie integrate sub forma unui “appliance” functional si sa nu fie declarate ca EoS (End of Sale) sau EoL |

| | |
|---|---|
| | (End of Life). De asemenea, ofertantul trebuie să facă dovada că echipamentele catalogate de producator nu sunt refolosite (“refurbished”); |
| | -Procesor multi-core care sa suporte rularea concurenta a multiplelor servicii; |
| Cerinte hardware obligatorii | -minim 1 GB memorie instalata, expandabila la minim 2 GB; |
| | -minim 512 MB memorie FLASH instalata, expandabila la minim 8 GB; |
| Interfete | -3 x interfete 10/100/1000 Gigabit Ethernet, pe placa de baza; |
| | -4 x sloturi externe de tip EHVIC, cu posibilitatea de echipare ulterioara; |
| | -2 x sloturi externe de tip USB 2.0; |
| | -2 x porturi consola (115,2 kbps) dintre care unul USB si altul serial; |
| | -1 x port auxiliar pentru administrare de la distant (115,2 kbps); |
| Performanta sistemului | -Viteza de rutare a pachetelor: minim 480.000 pps (cu pachete de 64 octeti); |
| | -Capacitate totala de procesare: minim 240 Mbps. |
| Functionalitatii minimale | -Suport pentru Policy Routing si QoS; |
| | -Suport pentru accelerare forward pachete; |
| | -Configurabil de la consola prin linie de comanda via SSH, telnet, configurabil web; |
| Protocoale si standarde | -Rutare statica; |
| | -OSPF, BGP si GRE; |
| | -Suport high availability (HSRP, GLBP sau echivalent) |
| | -IEEE 802.1q; |
| | -IEEE 802.1ag; |
| | -IEEE 802.3ab; |

| | |
|---|---|
| Parametri alimentare | -1 x sursa AC, compatibila cu standardele romanesti;<br>-Consum de putere fara POE: maxim 330W;<br>-Frecventa de functionare: 47-63Hz;<br>-Tensiune de functionare: 100 – 240 VAC;<br>-Curentul de functionare: maxim 3,4A (la 230V); |
| Mediu de functionare | -Temperatura de functionare: de la 0° la 40° C (la o altitudine de maxim 3000m)<br>-Umiditate: de la 10 la 85%. |
| Dimensiuni | -19” montabil in rack;<br>-Maxim 2 RU inaltime;<br>-Kit de rackare inclus;<br>-Greutate maxima: 14Kg |

## 8. Echipamente firewall cu VPN

**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 | 2 x interfete 10GbE SFP+ 8 x interfete 10/100/1000 Duale (RJ-45/SFP) 12 x interfete 10/100/1000 Ethernet<br>4 x interfete 10/100/1000 Ethernet cu bypass (functionare in pereche)<br>2 x interfete 10/100/1000 Ethernet pentru Management 2 x porturi USB<br>1 x modul stocare intern 128 GB |

| | |
|---|---|
| Performanta sistemului | Firewall Throughput(pachete UDP 1514 byte): 20 Gbps |
| | Firewall Throughput(pachete UDP 512 byte): 20 Gbps |
| | Firewall Throughput(pachete UDP 64 byte): 20 Gbps |
| | Firewall Throughput(pachete pe secunda): 31 Mpps |
| | IPSec VPN Throughput(pachete 512 byte): 8 Gbps |
| | IPS Throughput: 3.6 Gbps |
| | Antivirus Throughput(flow-based): 2.1 Gbps |
| | Antivirus Throughput(proxy-based): 1.7 Gbps |
| | Tunele IPSec VPN (gateway to gateway) concurente: 10000 |
| | Tunele IPSec VPN (client to gateway) concurente: 50000 |
| | Useri SSL-VPN: 3000 |
| | SSL-VPN Throughput: 350 Mbps |
| | Concurrent session(TCP): 7 Milioane |
| | New Session/Sec(TCP): 190000 |
| | Policies(Maxim): 100000 |
| | Domenii virtuale: 100 |
| | Configuratii redundante posibile: Activ/Activ, Activ/Pasiv, Cluster Unlimited Users Licences |
| Parametrii echipament | Alimentare alternativa 100-240V, 50-60Hz 2 x surse de alimentare redundante Hot-swappable |
| Protocoale si Servicii de Retea standarde | |
| | Rutare/Retea: Suport WAN multiplu Suport PPPoE Client/Server DHCP Policy-based routing |
| | Rutare dinamica IPv4/IPv6-RIP,OSPF,BGP,Multicast(IPv4) |
| | Suport multi-zone |

Rutare intre zonele de securitate

VLAN Tagging(802.1q) Rutare intre VLAN-uri Multi-link aggregation(802.3ad)

Suport IPv6 (Firewall,DNS,Transparent,SIP,rutare dinamica) Traffic

Shaping: Policy-based Suport DiffServ

Banda Garantata/Maxima/Prioritara Shaping per-IP,per-Account, per aplicatie Domenii

Virtuale: Domenii Firewall/Rutare separate Politici de securitate per domeniu Interfete VLAN separate High Availability:

Funcționare Activ/Activ, Activ/Pasiv Statefull Failover Link status monitor Link failover Server Load Balancing Servicii de Securitate Firewall: NAT,PAT,Transparent

Rutare dinamica-RIP,OSPF,BGP,Multicast Policy-based NAT Domenii Virtuale (NAT/Transparent) VLAN Tagging(802.1q) SIP/H.323/SCCP NAT Traversal

Profile granulare de protectie per-policy

Suport proxy explicit, optimizare WAN, caching Suport IPv6 VPN: PPTP,IPSec,SSL

Suport criptare DES,3DES,AES Autentificare SHA-1 / MD5 PPTP,L2TP,VPN Client pass through Suport VPN "Hub and Spoke" Autentificare IKE cu Certificate(v1 si v2) IPSec NAT Traversal

Intruziunilor Suport Anomalii de protocoale

Suport Semnaturi definite de utilizator Suport IPv6

Antivirus Protecție anti-malware (virus, troian, worm, spyware)

Protocoale: HTTP/HTTPS; POP/POP3S; SMTP/SMTPS; IMAP/IMAPS, IM (AIM, ICQ, Yahoo, MSN)

Blocare fisierelor in funtie de tip sau dimensiune Suport Ipv6

Antispam SMTP/SMTPS;IMAP/IMAPS;POP/POPS

Suport RBL/ORDBL Inspecție header MIME, filtrare dupa

| | |
|---|---|
| | cuvinte/expresii si black/white list<br><br>Update-uri automate şi în timp real. |
| Management | Administrare: Consola, Telnet, SSH, HTTP/HTTPS,CLI Utilizatori/Administratori cu drepturi configurabile<br><br>Syslog,SNMP,log-uri interne,grafice,notificari<br><br>email<br><br>Autentificare: Baza de date locala Integrare Active Directory Integrare LDAP/Radius/TACACS+ IP/MAC address binding |
| Software | Licente pentru activarea si actualizarea serviciilor Antivirus, Antispam, Prevenirea Intruziunilor,etc.(trebuie activate toate licentele posibile pe echipament) |

## 9. Echipament de protecție aplicații web

| **Denumire** | **Echipament virtual destinat protectiei aplicatiilor web** |
|---|---|
| Configurație | • Hypervisor suportat: Vmware ESXi, Microsoft sau echivalent<br>• Numar maxim de vCPU: 2<br>• Numar maxim de vNIC: 4<br>• Spatiu minimvirtual de stocare: 40GB<br>• Memorie minima virtuala: 1024MB |
| Caracteristici | • Trafic procesat: minim 100Mbps<br>• Numar de tranzactii HTTP per secunda procesate: 8.000<br>• Numar licente aplicatii: nelimitat |
| Moduri de instalare | • Transparent<br>• Transparent proxy<br>• Reverse proxy<br>• Offline |
| Optiuni de definire a politicilor si profileleor de securizare | • Definire in mod automat si dinamic a profilelor de securizare pentru aplicatii in urma monitorizarii traficului acestora.<br>• Wizard pentru politici de securizare si politici predefinite. |
| Optiuni pentru | • Operatiunea de autentificare trebuie sa poata verifica |

| | |
|---|---|
| autentificarea utilizatorilor | credentialele prin verificare locala, prin RADIUS, LDAP si NTLM. |
| Suport High Availability | • Optiune pentru clustering de tip Activ/Pasiv.<br>• Optiune pentru sincronizarea configuratiei cu procesare paralela a traficului intre doua sau mai multe echipamente. |
| Protectie la nivel de aplicatie | • Protectie impotriva atacurilor de tip:<br>Cross Site Scripting<br>SQL Injection<br>Session Hijacking<br>Cookie Tampering /Poisoning<br>Cross Site Request Forgery<br>Command injection<br>Remote File Inclusion<br>Forms Tampering<br>Hidden Field Manipulation<br>Outbound Data Leakage<br>HTTP Request Smuggling<br>Remote File Inclusion<br>Encoding Attacks<br>Broken Access Control<br>Forceful Browsing<br>Directory Traversal<br>Site Reconnaissance<br>Search Engine Hacking<br>Brute Force Login<br>Access Rate Control<br>Schema Poisoning<br>XML Parameter Tampering<br>XML Intrusion Prevention<br>WSDL Scanning<br>Recursive Payload<br>External Entity Attack<br>Buffer Overflow<br>Denial of Service<br>• Protectie DLP cu reguli predefinite si reguli configurabile.<br>• Protectie Anti Web Defacement.<br>• Validarea compliantei RFC HTTP a traficului procesat<br>• Functionalitate de scanare si raportare a vulnerabilitatilor aplicatiilor web protejate.<br>• Suport pentru aplicatiile Microsoft Exchange,SharePoint, ActiveSync |

si protocolul RPC over HTTP.

| | |
|---|---|
| Optiuni de procesare a traficului | • Load balancing la nivel de aplicatie.<br>• Compresie a datelor.<br>• SSL offloading. |

## 10.Infrastructura telefonie

Toate componentele centralelor telefonice trebuie sa fie fabricate de aceelasi producator.

### 1. Centrale telefonice locale

Cerinte tehnico-functionale minime:

- sistem hibrid care suporta atat telefonie normala TDM (analogic si digital), telefonie fara fir tip DECT si Voice over IP (VoIP) in orice combinatie posibila;
- compatibila cu standardul de comunicatie SIP (Session Initiated Protocol), echipare actuala cu 4 trunchiuri SIP
- permite pana la 200 de linii externe (ISDN, analogice, IP), pana la 512 extensii (interioare) digitale, pana la 512 extensii (interioare) analogice, pana la 512 extensii IP in oricare dintre combinatii fara a exista limitari la numar de porturi analog/digiatl/IP sub limita de 512
- configuratia ofertata permite minim 12 linii externe analogice cu CLIP in configuratia ofertata;
- configuratia ofertata suporta networking cu minim 256 de centrale interconectate cu o transparenta de 95%, cu minim 32 canale IP pentru interconectare networking cu alte sisteme;
- echipare mesagerie vocala integrata min 16 canale simultane, memorie de inregistare ce acopera minim 0,5 ore / post telefonic si optiunea de „call center”, cu posibilitate de inregistrare a convorbirilor telefonice 32 ore;
- contine 16 canale simultane pentru mesaj de intampinare in minim 8 limbi simultane;
- Configuratia ofertatat trebuie sa suporte conturi personale (parole pentru acces extern) minim 2000 de account coduri

Alte facilitati standard minime obligatorii:

- Call-Forward-Redirectarea apelurilor de la aparatul propriu la un alt interior.
- Follow me-Preluarea apelurilor altui interior la aparatul propriu.
- Do not disturb-Nu deranjati-Realizeaza doar blocarea apelurilor telefonului respectiv.
- Grup hunting-Comutarea secventiala a apelurilor grupului dupa o anumita regula (liniar/ciclic).
- Pick-up-Preluarea apelurilor altui aparat din grup.Pentru fiecare apel se formeaza codul de preluare.
- Reapel automat-apelarea automata a unei extensii cand aceasta devine libera sau daca aceasta nu a raspuns.
- Apeluri de grup - apel simultan la mai multi utilizatori.
- Apel inlantuit - apelarea consecutiva a mai multor extensii din grup dupa un timp prestabilit daca apelul nu a fost preluat.
- Semnalizarea sonora distincta a apelurilor pentru apeluri interne, externe, reapleuri sau revenire apeluri.

- ARS sau LCR (Least Cost Routing)-Selectare automata a rutei pentru un apel extern.Este aleasa linia/interfata cea mai putin costisitoare in functie de destinatia apelului (GSM, VoIP-international, local, interurban)
- Sa suporte facilitate extensii de tip Manager/Secretara
- configuratia ofertata trebuie sa permita conectarea a minim 8 telefoane digitale, minim 20 telefoane analogice, minim 8 telefoane IP, 20 casute de voice mail
- sa suporte aplicatie de Call Center cu pana la 512 agenti si 64 grupe de ACD (Automated Call Distribution);
- sa fie echipata cu CLIP FSK / DTMF pentru liniile externe si interne;
- sa suporte TAPI 2.0 3rd party si 1st party;
- sa permita restrictionarea apelurilor intre departamente;
- sa suporte cel putin 8 moduri de functionare (Zi, Pauza1, Pauza2, Noapte, Weekend, Sarbatori legale, Program flexibil angajati, etc);
- sa suporte functia de integrare a telefoanelor mobile in sistem;
- sa fie prevazuta cu software pentru contorizare si administrare telefoane;
- sa suporte pana la 64 circuite de conferinta;
- tensiune de alimentare 110 V AC / 230 V AC / 50 Hz / 60 Hz;
- consum total energie maxim 450 W;
- dimensiuni de gabarit carcasa: maxim 89 (Î) x 432 (L) x 392 (A) mm;
- greutate: maxim 0.2 kg pentru unitatea neechipata; maxim 275 grame / card de extensie;
- compatibil standarde IEEE 802.3 10 Base-T, respectiv 100 Base-T, autonegociere;
- protocol comunicatie tip CSMA / CD;
- minim 4 porturi pentru comunicatia prin LAN pentru router intern centrala;
- posibilitatea definirii de tabele de rutare pe baza carora sistemul cauta traseul cel mai ieftin (putin costisitor) pentru apelurile care pleaca din locatie la anumite intervale orare;
- Management centralizat via web cu multi level autentification pentru intreg sistemul de comunicatii viitor dar si existent cu urmatoarele facilitati :
    - Alarm handling si diagnoza full
    - On-line junal
    - Operational Maintenance
    - Schimbari si modificari
    - Facilitati extensii si trunchiuri
    - Clase de traffic
    - Local/remote read si software identification
    - Profile de user
    - Protectie prin parole in functie de nivelul de acces
    - SNMP
    - System identification
    - Test call cu diagnoza

    - Trafic measurement
- sa ofere posibilitati variate de adaptare a tuturor proceselor de comunicatii la fluxurile de activitate (workflow) ale institutiei, optimizandu-le (gestionare prin intermediul unui PC sau prin LAN);
- posibilitatea integrarii cu sistemele locale existente;
- sa fie prevazuta cu minim 2 posturi de interfon ce se cupleaza la centrala telefonica (cu alocare de numar);
- sa fie prevazuta cu un echipament separat ce asigura protectia in cazul aparitiei unei suprasarcini (trasnet, variatii mari ale tensiunii de alimentare, etc.).

## 2. Centrala telefonica IP

Caracteristici generale obligatorii:

Sistemul de comunicatii de tip full IP care va face posibile comunicatiile de voce ale aplicatiei de Call Center, va fi de tipul redundant active-activ in minim doua noduri, bazat pe tehnologia "virtual machine fault tolerant, level 3 ", astfel nu vor exista intreruperi de voce sau de aplicatii, creind o disponibilitate de 100% a tuturor extensiilor sistemului de comunicatii.

Administarea tuturor componentelor de telefonie de tip IP-PBX (Servere de voce, telefoane IP, IVR, ACD) cat si a sistemelor existente se va realiza in mod centralizat intr-o singura interfata de administare unica de tip web.

Sistemul de operare pentru serverele de comunicatii ofertate trebuie sa fie la ultima versiune comerciala de pe piata si sa faca parte din categoria sistemelor de operare consacrate, exemplu: MS Windows, Linux, etc.

Hardware-ul ofertat pentru server-ul de comunicatii trebuie sa fie dedicat, nefiind inclus in solutia de tip blade ceruta pentru celelate componente ale sistemului.

Aplicatii si facilitati suportate de catre servere:

- Announcement services – Voice Processing – Unified Messaging – Voice Mail – Interactive Voice Response (IVR)
- Automatic Call Distribution (ACD), sistemul de comunicatii va directiona apelurile automat catre agenti in cazul in care Call Center-ul nu este disponibil.
- DTMF over IP
- Computer Telephony Integration (ECMA CSTA and TAPI 2.1) cu facilitatie de mai jos suportate
    - Call answer - Call diversion
    - Call back – pentru coada de asteptare din Call Center
    - Diversion, Fallback reason
    - Group manipulating Group monitoring
    - Hold call

        - Maintenance event reporting
        - Message waiting
        - Twinning
    - Convergenta Fix to Mobile
    - FAX over IP (Pass-Through si Fax Relay)
    - IP-DECT/VoWLan cordless communication
    - Messaging
    - Management centralizat via web cu multi leve autentificatio pentru intreg sistemul de comunicatii viitor dar si existent cuurmatoarele facilitati :
        - Alarm handling si diagnoza full
        - On-line junal
        - Operational Maintenance
        - Schimbari si modificari
        - Facilitati extensii si trunchiuri
        - Clase de traffic
        - Local/remote read si software identification
        - Profile de user
        - Protectie prin parole in functie de nivelul de acces
        - SNMP
        - System identification
        - Test call cu diagnoza
        - Trafic measurement
    - Intre cele doua servere va fi prevazut un mediu de virtualizare de tip Marathon everRun® MX 6.0 sau VMware vSphere Hypervisor.
    - Suport FAX T.38 (H.323, MGCP, si SIP);

Facilitati suportate de catre extensii (interioare) IP:

- Abbreviated dialing: – individual – per user group – common pool
- Automatic ring back(COB): – on busy – on next use – cancel ARB – multiple ARB – ARB protected – ARB after diversion(s)
- Break-in-protection: – party (ticker-tone) – break-in protection
- Call forwarding: – unconditional (follow-me) – on no answer – when absent – when busy –

when not reachable – multi-hop call diversion
- Call waiting indication – COB by destinaton
- Call hold (start enquiry)
- Camp-on busy: – automatic (destination profile) – call offer (originator profile) – music on camp-on busy
- Connected Party Display
- Cost Centre Dialling
- Distinctive ringing : – intre apeluri interne– apeluri externe – automatic ring back – emergency call – message waiting
- Desk sharing, o extensie IP se poate muta la alt telefon si prin introducerea parolei la noul telefon are facilitatie de la telefonul propriu.
- DDI barred
- Do not disturb: – routing to operator – user deactivation – deactivation after time
- Plan de numerotatie de 12 digiti in intrega reatea proprie
- Message-waiting indicator
- Number-presentation restriction
- Transfer before answer (new party)
- Twinning
- User-to-user text messaging
- Terminalele IP vor acccepta adrese IP via DHCP

Facilitati suportate de catre grupuri de extensii (interioare):

- Absent-status indication (LED, display(icons))
- Announcements on empty group
- Call diversion on empty group
- Call pick-up: – individual extension – group call – unrestricted
- Camp-on busy queuing
- Chaining of group diversions
- Do not Disturb
- Follow-me
- Group follow-me
- Group hunting mechanism: – cyclic (round-robin) – linear (home hunting) – parallel (multiple ringing)
- Group park
- Group status display
- Monitoring absent/present status
- Monitoring idle/busy/ringing status
- Music-on-Hold
- Private Park

Facilitati suportate de catre extensii (interioare) de tipul Mobility:

- Abbreviated dialling
- Add-on conference
- Automatic ring back
- Automatic trunk find
- Break-in

- Call forwarding
- Call pick-up
- Camp-on busy
- Call waiting indication (acoustical)
- Calling Number Display
- CSTA
- DDI barred
- Desk sharing
- Dialled intercom
- Do not disturb
- Enquiry/call hold
- FDCR/toll ticketing
- Follow-me
- General facility cancel - Group member (e.g. ACD group, Executive/Secretary group, etc.)
- Hotline
- Last External Number Repeat
- Malicious-call trace
- Message waiting (acoustical)
- Multi-party conference (up to 8 users)
- Multi-party listen in (up to 15 users)
- Music on hold
- Operator assistance
- Password dialling
- Personal identification dialling
- Post-dialling
- Selective diversions, distinguishable betweeninternal and external callers
- Secret call
- Shuttle/transfer
- Single Digit Dialling
- Traffic-class selection
- Traffic-class assignment
- Twinning
- Voice logging

Facilitati suportate de extensii (interioare) de tip Manager/Secretara:

- Absent overrule by secretary
- Absent/present switching by: – manager – secretary
- Alternative secretary: – break-in override – absent overrule
- Break-in override by secretary - Break-in protection
- Call diversion to secretary on busy/absent
- Camp On Busy
- Intercom call
- Multi-call park (multi-hold)
- Multi manager/multi secretary arrangements - Multi-line answering: – selective answering – internal/external call indication
- Private number
- Status monitoring: – busy/idle/ringing – absent/present

- Wite list

Facilitatile sistemului de comunicatii pentru linii externe (trunchiuri):

- Alternative routing on congestion
- Barring external numbers
- Bundle splitting
- DDI-fail diversion on: – ringing time-out – number-unknown – busy extension – unsuccessful DDI call
- Default CLI
- Digit conversion
- Incoming DDI traffic: -digit conversion – DDI-fail to operator
- Least Cost Call Routing: – time-of-day – class of service – per user type (normal, priority or operator)
- Mobility Access
- Number analysis per trunk group
- Overflow on outgoing routes: -Time-break, budget-break protected
- Toll-ticketing

Facilitatile sistemului de comunicatii pentru linii externe (trunchiuri) SIP:

- Basic Call handling (RFC 3261)
- CLI and name display (RFC 3261)
- Diversion Header (draft-levy-SIP-diversion-08)
- DTMF support (RFC 2833)
- Fax (T38, G711)
- Payload formats in SDP (RFC 3555)
- QoS IEEE 802.1Q
- Registration/Authentication (RFC 2617, 3216, 3261 section 22)
- SDP handling (RFC 2327, RFC 3264)
- Secure Realtime Transport Protocol (SRTP)(RFC 3711)
- Session Guarding (RFC 4028)
- SIP reliability (RFC 3262)
- Transport Layer Security (TLS) (RFC 2246)

Facilitatile sistemului de comunicatii pentru inregistrare convorbiri:

Inregistrarea convorbirilor telefonice se va face prin crearea de catre serverul de comunicatii a unei locatii in cadrul sistemului unde vor fi stocate convorbirilor telefonice fara a folosi hardware suplimentar, creeindu-se astfel si redundanta inregistrarii convorbirilor.

Aplicatia de inregistrare convorbiri va avea urmatoarele facilitate obligatorii:

- Interfata usor de utilizat tip ribbon
- Preluare convorbiri din serverul de comunicatii
- palyer pentru fisiere . wav incorporat
- Posibilitate de trimitere inregistrare convorbire via email
- Permite diverse filter dupa: data, ora, tip inregistrare interior/exterior CLIP, numar format, trunchi

Codecuri suportate de catre extensii:

- Audio: G.711 (mu-law, a-law), G.722, G.722.1, G.729A / B, GSM-EFR, GSM-FR, ILBC, wideband audio;
- Video: H.261, H.263, H.264, si Wideband Video Codec;
- SIP (RFC 3261)

Securitate si caracteritici de retea:

Fiecare telefon va fi prevazut cu un buton prin care se poate face blocarea acestuia, accesul la telefon fiind protejat prin parola.

- Encryption (TLS, SRTP)
- RFC 2246 “TLS Protocol Version 1.0”
- RFC 3711 The Secure Real-time Transport Protocol (SRTP).
- LLDP-MED
- Suporta NAPT traversal
- Power: conform 802.1x
- RFC 2716 EAP-TLS.
- RFC 2865—2868 RFC’s related to 802.1x.
- RFC 3748 Extensible Authentication Protocol (EAP)
- RFC 5247 Extensible Authentication Protocol (EAP) Key Management Framework

Scalabilitate si performante obligatorii pentru sistem de comunicatii:

- Arhitectura redundanta scalabila pana la 15 noduri bazata pe “Virtual machine” cu posibilitatea balansarii incarcarii si asigurarii redundantei procesarii apelurilor;
- pana la 5000 telefoane inregistrate simultan pe system, din care 2500 pot fi de tip IP-Dect
- pana la 45000 de telefoane inregistrate simultan intr-o retea;
- pana la 600 de trunchiuri SIP
- Performante sistem 100.000 h BHCAs
- Trafic: 3000 Erlang
- Disponibilitate sistem: 99,99 %

Echipare sistem de comunicatii:

- Numar total Servere conform specificatii: 2
- Numarul total de trunchiuri SIP conform specificatiilor: 60
- Numarul total de extensii IP conform specificatii: 100
- Numarul total de extensii mobile: 20
- Numarul total de telefoane IP Dect conform specificatii: 4 bucati
- Mumart total de antene IP-Dect: 2 bucati

## 11.Aparate telefonice

### 1. Aparate telefonice digitale:

- Display LCD maxim168 x 58 mm cu posibilitate lumina display;

- Constructie modulara si adaptabila: 12 taste programabile cu posibilitate de upgrade la 32, posibilitate montare display suplimentar ,
- Receptor de telefon cu Bluetooth cu raza de functionare de 50 m si cu aceleasi facilitati ca si telefonul digital;
- Tastatura luminata;
- Taste rapide: Agende, Voicemail, Mesaj in asteptare, Retro apel, Conferinta;
- Tasta meniu: istoric apeluri, agenda, setari display, volum sonerie, lumina fundal;
- Handsfree, full duplex;
- Suporta casca;
- Taste de sistem usor de utilizat / indicatii pe display;
- Agenda de sistem 1000 numere / agenda de grup / agenda personala pentru 600 telefoane;
- Taste navigare;
- Istoric apeluri;
- Posibilitate de montare pe perete;
- Dimensiuni maxime: (l x L x a) 179 × 258 ×112 mm;
- Greutate max 1.3 kg;
- Temperatura de functionare minim intervalul 10 - 45 grade C; umiditate 10 -90 %;

**2. Aparate telefonice analogice:**

- display LCD cu 24 caractere,
- handsfree fullduplex,
- afisare numar apelant,
- 10 taste suplimentare programabile,
- posibilitate de montare pe perete,
- Dimensiuni maxime: (l x L x a) 215 x 237 x 58 mm;
- Greutate: maxim 0.8 kg;

- Temperatura de functionare minim intervalul 10 - 45 grade C; umiditate 10 -90 %;

**3. Aparate telefonice tip IP:**

- Display LCD maxim 168 x 58 mm luminat;
- Constructie modulara si adaptabila: 12 taste programabile cu posibilitate de upgrade la 32, posibilitate montare display suplimentar;
- Tastatura luminata;
- Taste rapide: Agende, Voicemail, Mesaj in asteptare, Retro apel, Conferinta;
- Tasta meniu: istoric apeluri, agenda, setari display, volum sonerie, lumina fundal;
- Tasta blocare telefon printr-o singura atingere si deblocare cu parola;
- Handsfree, full duplex;
- Suporta casca;
- Taste de sistem usor de utilizat / indicatii pe display;
- Agenda de sistem 1000 numere / agenda de grup / agenda personala pentru 600 telefoane;
- Taste navigare;
- Istoric apeluri;
- Posibilitate de montare pe perete;
- Interfata XML – posibilitate integrare cu alte aplicatii;
- Securizare convorbire;
- Posibilitate de integrare cu Microsoft Outlook;

- Dimensiuni maxime: (l x L x a) 179 × 258 ×112 mm;
- Greutate max 1.3 kg;
- Sa suporte PoE
- Temperatura de functionare minim intervalul 10 - 45 grade C; umiditate 10 -90 %;

**4. Aparate telefonice tip IP-Dect:**

- TFT grafic Display 158x126 Pixeli (260k);
- Meniu in limba Romana
- Indicator de ora si data care vor fi preluate din PBX
- Timp de conversatie minim 12 ore
- Timp de standby minim 120 ore
- Taste navigare
- Speaker automat sau manual
- 20 Melodii in functie de apleant
- Vibratii
- Istoric apeluri pentru ultimele 40 apleuri interior/exterior;
- Primire si trimitere de mesaje TEXT
- Tasta SOS predefinita;
- Integrare cu aplicatia de Call Center prin afisare status agenti
- Greutate maxima admisa 90 grame

## 12.Echipamente desktop PC

Dispozitivul trebuie sa asigure accesul la o infrastructură desktop virtuală via conexiune Ethernet.

Alimentarea trebuie sa fie integrată în terminal. Terminalele trebuie sa fie compatibile cel putin cu solutiile de virtualizare pentru desktopuri Microsoft Hyper-V, Citrix XenDesktop si Vmware View. Accesorii la terminale: mouse si tastatura.

| **Componenta** | **Cerinta tehnica minimala** |
|---|---|
| Diagonala ecranului | Minim 22” (55.9 cm) |
| Format | 16:9 |
| Contrast | 1000:1 |
| Luminozitate | 250 cd/m2 |
| Rezolutie | 1680 x 1050 pixeli |
| Unghi de vizualizare (orizontal/vertical) | 170°/170° |
| Timp de raspuns | Maxim 20 ms |

| | |
|---|---|
| Difuzoare | Minim 2 x 1.5W |
| Porturi integrate | 1 x DVI-I pentru atasarea unui al doilea display<br>1 x audio in<br>Minim 4 x USB 2.0<br>1 x RJ45 cu suport pentru Power over Ethernet (PoE) |
| Ergonomie | Inclinare: -5° / +35° |
| Mouse | 2 butoane, facilități de scroll |
| Consum | In operare in mod ECO: max. 34W<br>In operare la luminozitate maxima: max 39W |
| Suport hypervizori | Microsoft Hyper-V, Citrix XenDesktop, VMWare |
| Software inclus | Aplicatie software pentru administrarea terminalelor, cu cel putin urmatoarele functionalitati:<br>• Acces prin interfata web<br>• Identificarea si inventarierea terminalelor<br>  • Controlul starii dispozitivului (pornire/oprire/stand-by)<br>  • Restrictionarea accesului dispozitivelor catre infrastructura de desktop-uri virtuale<br>• Brokerajul conexiunilor<br>  • Servicii de autentificare a utilizatorilor via Microsoft Active Directory<br>  • Conectarea utilizatorilor la masinile virtuale<br>  • Session roaming (conectarea la o masina virtuala de la oricare terminal, folosind aceeleasi date de autentificare)<br>• Administrarea desktop-urilor virtuale<br>  • Definirea unor colectii de desktop-uri<br>  • Creerea de desktop-uri plecand de la un sablon<br>  • Autorizarea utilizatorilor si a grupurilor de |

| | |
|---|---|
| | utilizatori |
| | pentru accesul catre desktop-urile virtuale<br>• Monitorizarea starii desktop-urilor virtuale |
| | Aplicatia va include licentele necesare pentru toate terminalele ofertate. |
| Certificari | Certificare CE conform EC 2004/108/EEC<br>FCC Class B<br>RoHS<br>WEEE |

## 13.Echipamente laptop

Următoarele cerințe sunt minime și obligatorii

| Componenta | Descriere configuratie minimala |
|---|---|
| Chipset | Mobile Intel QM77 Chipset sau echivalent |
| Procesor | Intel Core i3-3110M Processor (2.4 GHz, 3 MB cache) sau echivalent |
| Memorie instalata | Min 4GB DDR3 non ECC |
| Memorie maxima | Max. 16GB |
| Placa video | Placa video integrata |
| HDD | Min 320GB SATA 7200 RPM |
| Unitate Optica | DVD-RW in compartiment modular, interschimbabil cu alte accesorii (a doua baterie, al doilea hard disc) |
| Audio | Boxe stereo integrate |

| | |
|---|---|
| | Doua microfoane integrate |
| | headphone/line out |
| | stereo microphone in |
| Display | Min 15.6” TFT LED HD display , anti glare, |
| | Full HD Webcam integrata |
| Carcasa | Rezistenta la socuri |
| Comunicații integrate(nu se accepta adaptor) | placa de retea integrata Gigabit (10/100/1000 Mbps ) |
| | 802.11a/b/g/n WLAN |
| | Bluetooth 4.0 |
| | Kit antenna UMTS/LTE |
| Tastatura | Cu bloc numeric |
| Pointing Device | Touchpad |
| | Touchstick |
| Interfete I/O integrate (nu se accepta adaptor) | - 1 x DisplayPort- 1 x ExpressCard/54 slot |
| | - 1 x SmartCard slot |
| | - 1 x MemoryCard slot (SD, MS, MSPRO, SDHC, SDXC) |
| | - 1 x SimCard slot. Optional, UMTS module for HSDPA |
| | - 1 x LAN RJ-45, 1 x VGA |
| | - 2 x USB 2.0 (thereof 1 x USB/eSATA combo), 2 x USB 3.0 |
| | - 1 x serial port |
| | - 1 x headphone, 1 x microphone |
| | - 1 x DC-in |

| | |
|---|---|
| | - 1 x Docking connector |
| | - 1 x Kensington Lock |
| Baterie | - 6 cell high capacity Li-Ion |
| | - Autonomie pana la 10 ore cu o singura baterie (conform rezultatelor obtinute cu MobileMark2007) |
| | - posibilitate de a folosi 2 baterii. Autonomie pana la 17 ore cu ambele baterii instalate. |
| | Adaptor AC inclus |
| Caracteristici de securitate si management | Chip/modul de securitate integrat pe placa de baza tip TPM care ofera posibilitatea criptarii datelor atat hardware cat si software |
| | Aplicatie de monitorizare si management local si de la distanta, dezvoltata de producatorul sistemului de calcul, cu cel putin urmatoarele functionalitati : |
| | Management de la distanta atat online cat si offline |
| | Rapoarte detaliate despre componentele sistemului |
| | Bios management |
| | Remote power management |
| | Aplicatie software integrata in BIOS-ul statiei de lucru, accesibila fara a porni sistemul de operare, care sa permita stergerea securizata a datelor prin suprascrierea acestora folosind cel putin trei algoritmi: 1 suprascriere, 7 suprascrieri (DoD 5220.22-M ECE) sau 35 suprascrieri (Guttman) |
| | Cititor de amprente (fingerprint reader) integrat |
| Greutate | Max 2,5 Kg |
| Sistem de operare | Windows 7 Professional OEM preinstalat, CD/DVD pentru restaurarea sistemului |
| Conformitate cu standarde europeene | ROHS / WEEE, Energy Star 5.0, WiFi certified, EPEAT Gold |

| | |
|---|---|
| Conformitate cu ISO 9001, standardele privind managementul calitatii | |

## 14.Echipament pentru recunoașterea semnăturii olografe

**Cerinte functionale**

Solutia va include o platforma pentru recunoasterea semnaturii olografe in scopul asigurarii unei protectii sporite in zona utilizatorilor interni cu drept de administrare de continut (adaugare/stergere/modificare) in cadrul Portalului. Acest continut vizeaza domenii precum: instructiuni de utilizare a Portalului, date cu caracter personal etc. Platforma va solicita astfel acestor utilizatori, in mod suplimentar, semnatura olografa la fiecare incercare de autentificare cu nume utilizator si parola.

**Cerinte tehnice minime și obligatorii**

| | |
|---|---|
| Tip senzor | Active Electromagnetic |
| Tip Stilou | Active Energized |
| Suprafata pentru semnare | Maxim 113 x 34 mm |
| Rata de conversie a datelor | Minim 376 puncte/s |
| Rezolutie semnatura | Minim 410 true points/inch |
| Conectivitate | USB, Serială, ethernet |

## 15.Dispozitive token

Pentru partea de autentificare multi-factor a utilizatorilor interni, solutia prevede o platforma formata din echipamente token si clientul software (local) aferent. Echipamentele token tip oferite vor indeplini urmatoarele caracteristici tehnice minime:

- Standarde suportate: ISO/IEC 7816 1-2-3, Global Platform 1.4
- Certificate: FIPS 140-2 Level 3 si Common Criteria EAL5+
- Standarde criptografice suportate: DES/3DES, AES, SHA1, RSA 1024-2048
- Token-urile trebuie sa suporte tehnologiile: JavaCard, PKCS#11/MS CAPI
- Integreaza in cip un procesor de inalta performanta pentru generarea cheilor criptografice
- Capabilitatea de a genera coduri OTP time-based si event-based (One Time Passwords)
- Memorie EEPROM: 64KB
- Cicluri de rescriere: 500.000
- Conforme cu standardul IEC-1000-462 level 4 pentru descarcari electrostatice: 15KV (aer)/

8KV (contact)

- Compatibile cu sisteme de operare: Windows XP, 2000, 2003 Server, Vista, Windows 7, Linux, Mac OS
- Conforme cu specificatiile: USB 2.0, CCID
- Certificate FCC, CE, UL, RoSH

## 16.Echipament multifuncțional pentru imprimare și scanare

| | |
|---|---|
| Tehnologie | Laser |
| Viteza de imprimare | 23ppm color/ 23 ppm alb-negru |
| Rezolutie de imprimare | 600 x 600 x 4 dpi |
| Limbaj de tiparire | Adobe PostScript 3, PCL 6 |
| Format | A4 |
| Procesor | 533 Mhz |
| Memorie standard/maxim | minim 256 MB / 768 MB max. |
| Timp de tiparire a primei pagini | 12 secunde color / 12 secunde alb-negru |
| Copierea primei pagini | 20 secunde color / 13 secunde alb-negru |
| Rezoltie copiere | 600 x 600 dpi |
| Timp de incalzire | maxim 31 sec |
| Conectivitate | USB 2.0, 10/100 Base-TX Ethernet |
| Fax | 33.6 Kbps, 200 numere apelare rapida, rezolutie 400x400 dpi |
| Scanare | 1200x1200 dpi |
| Destinatii de scanare | email, FTP, SMB , USB |
| Formate fisiere scanate | PDF, JPEG, TIFF, Multi TIFF |
| Alimentare cu hartie din tava | minim 250 coli, posibilitate marire capacitate hartie pana la 500 coli |
| ADF | minim 35 coli |
| Capacitate iesire hartie | minim 150 coli |
| Greutatea maxima a hartiei | 60 – 216 gsm |
| Dimensiuni acceptate | de la 76 x 127 mm pana la 216 x 356 mm |
| Tipuri de hartie acceptata | hârtie normala, lucioasa, carti de vizita, plicuri, etichete, carduri |
| Suport drivere | Windows 2000/XP/Vista, Server 2003/2008, Mac OS 10.5, Linux |
| Volum maxim de tiparire lunar | minim 40,000 pagini |
| Securiate | Secure HTTPS (SSL), IPsec, Autentificare 802.1x, IPv6, SNMPv3, filtrare adrese IP |

# 10.Cerinte privind software-ul licențiat

## 1. Software portal

**Software-ul trebuie sa indeplineasca urmatoarele cerinte minime si obligatorii:**

- sa puna la dispozitie unelte avansate de dezvoltare rapida de site-uri
- sa aiba capabilitati avansate de Web Content Management System pentru a permite dezvoltarea rapida de functionalitati de tip colaborativ
- sa aiba un set bogat de functii de baza care sa permita devoltarea rapida de noi aplicatii
- sa puna la dispozitie unelte de editare si gestiune a continutului
- sa puna la dispozitie unelte de raportare analitica si de performanta
- sa aiba capabilitati de scalare si web-caching
- sa puna la dispozitie un sistem de taxonomie cu numar nelimitat de termeni ce sa fie asociati modulelor si paginilor dezvoltate
- sa puna la dispozitie un sistem care sa permita definirea de etichete custom pentru pagini si module

**Functionalitati specifice:**

**Software-ul** trebuie sa:

- puna la dispozitie o interfata de administare care sa permita dezvoltarea rapida de versiuni ale siturilor web pentru dispozitive mobile
- integreze functionalitati "Google Analytics" privind traficul pe situl web de pe dispozitivele mobile
- sa puna la dispozitie unelte de previzualizare a sitului web pe dispozitive mobile
- sa detecteze automat cand situl web este accesat de pe un dispozitiv mobil si sa redirecteze accesul catre continut optimizat pentru astfel de tipuri de dispozitive
- sa puna la dispozitie sabloane de situri web optimizate pentru vizualizare pe dispozitive mobile

**Software-ul** trebuie sa puna la dispozitie:

- mecanisme prin care utilizatorii non-tehnici sa poata edita continutul direct pe web, fara suport IT
- o bara de menu de tip "ribbon" cu optiuni de adaugare si editare de continut
- un sistem de fluxuri de aprobare a continutului structurat pe ierarhia organizationala a beneficiarului. Fluxurile de aprobare sa poata avea un numar nelimita de stari si de aprobatori
- mecanisme intrinseci pentru crearea si gestionarea rapida de profile personale de utilizator si tablouri de bord
- un sistem intern de mesagerie care sa permita utilizatorilor sa trimita si sa primeasca mesaje personale
- un director intern cu membrii siturilor dezvoltate
- un framework care sa permita creare de servicii web
- mecanisme de integrare cu servicii de tip cloud
- mecanisme avansate de cautare in cadrul siturilor care sa includa minim urmatoarele tipuri: Boolean, dupa fraza, dupa relevanta, folosind caractere "Joker", fuzzy
- mecanisme de configurare prin intermediul fisierelor de configurare
- mecanisme de publicare multi-limba a continutului

- mecanisme de caching a continutului
- mecanisme de schimbare a aparentei sitului
- mecanisme de auditare a intregii activitati de modificare a siturilor dezvoltate
- mecanisme de verificare a integritatii fisierelor sistemului
- mecanisme de verificare a disponibilitatii siturilor

Software-ul trebuie sa includa functionalitati avansate de gestiune a documentelor care sa permita stocarea, controlul si vizualizarea documentelor.Gama de documente gestionate sa cuprinda fisiere multimedia (filme, imagini etc) iar acestea sa poata fi vizualizate cu sau fara metadatele asociate.

**Functionalitatile trebuie sa includa:**

- definirea de dosare structurate ierarhic cu numar nelimitat de niveluri de imbricare
- posibilitatea de grupare logica a documentelor cu numar nelimitat de grupari
- posibilitatea de stocare a documentelor atat intern, in cadrul sistemului, cat si in afara acestuia, folsind servicii de tip cloud private
- posibilitatea de definire de drepturi de acces la nivel de document si/sau dosar care sa includa minim: adaugare, stergere, editare, vizualizare
- mecanisme de versionare a documentelor
- fluxuri de aprobare a documentelor inainte de publicare
- mecanisme de raportare statistica privind download-ul de documente
- mecanisme de creare de biblioteci de documente pornind de la zero sau de la biblioteci pre-existente
- mecanisme de blocare a posibilitatilor de download a documentelor

## 2. Software colaborativ de tip CRM

### 1. Cerințe tehnice generale

Sistemul de gestionare a sesizarilor trebuie sa indeplineasca urmatoarele functionalitati:

- Solutia trebuie sa functioneze pe o arhitectura n-tier.
- Solutia trebuie sa foloseasca o baza de date relațională.
- Sa poata fi accesata prin browser fara a fi necesara instalarea de software aditional sau licente pe statiile de lucru ale utilizatorilor.
- Arhitectura solutiei trebuie sa asigure redundanta.
- Solutia trebuie sa dispuna in standard de un modul de help integrat in interfata utilizator.
- Solutia va dispune de un editor bazat pe tehnologie web în vederea definirii machetelor aferente formularelor web noi sau pentru modificarea celor existente, cu ajutorul căruia să se poata marca prin placeholdere poziționarea atributelor entităților necesare a fi folosite pe formular; totodata este necesar ca aceasta opțiune să ofere posibilitatea adăugării unor zone dinamice, multiplicabile la runtime(de exemplu, pentru a simula rânduri multiple în cadrul unui tabel), setării unor input mask-uri pentru anumite câmpuri din cadrul formularului, sau a setării unor expresii regulate în vederea validării
- Solutia va permite modificarea formularelor web existente și definirea de noi formulare, fără intervenția furnizorului, fără a scrie cod sursă suplimentar și fără a afecta datele colectate deja în baza de date
- Solutia va dispune de o interfață generică pentru achiziția de date din alte sisteme/aplicații informatice externe; sistemul va centraliza aceste informatii, in functie de modelele informationale create.
- Solutia va permite definirea de nomenclatoare necesare modelelor informationale ale

documentelor create, precum si gestiunea valorilor din cadrul acestora.

- Solutia trebuie sa se integreze complet cu solutia de management al utilizatorilor: prin transferul proprietatilor utilizatorului catre aplicatia de de suport informational. Accesul utilizatorilor in solutia de gestiune a tichetelor se va face prin recunoasterea automata a credentialelor.
- Interfata utilizator complexa (managementul si introducerea datelor prin liste, lupe, pick lists etc).
- Solutia trebuie sa ofere in standard functionalitatea de atasare a fisierelor in cadrul inregistrarilor.
- Solutia trebuie sa ofere in standard functionalitati de detectie si de rezolvare a elementelor duplicat.
- Administratorul trebuie sa poata stabili regulile de detectie a duplicatelor pe inregistrarile de tip persoana, institutie. Detectia duplicatelor trebuie sa fie aplicabila si la importul de date prin interfata web.

Solutia trebuie sa fie scalabila si sa permita extensia cu diverse module;

### 2. Cerinte specifice de securitate si management al utilizatorilor

- Solutia trebuie sa ofere o interfata web de administrare a utilizatorilor.
- Definirea utilizatorilor trebuie sa poata fi facuta si in modul multiplu (introducere prin selectarea multipla a utilizatorilor disponibili si atribuirea acestora a unui rol de securitate implicit).
- Utilizatorii solutiei trebuie sa poata avea unul sau mai multe roluri de securitate.
- Utilizatorii trebuie sa poata fi grupati in entitati functionale in organizatie, in echipe, teritorii, locatii si in grupuri de resurse. Un utilizator trebuie sa poata face parte din mai multe echipe simultan (infiintare de echipe virtuale de lucru).
- Solutia trebuie sa permita definirea de utilizatori de tip “Read Only” sau definirea de utilizatori de tip “Administrator” (userii de tip Administrator trebuie sa aiba acces doar la functiile de administrare si sa nu utilizeze din licentele achizitionate).
- Solutia trebuie sa ofere in standard functionalitatea de reasignare din interfata web a inregistrarilor atribuite unui utilizator (in vederea preluarii responsabilitatii de catre un inlocuitor).
- Solutia trebuie sa permita gruparea utilizatorilor pe baza rolurilor si restrictionarea accesului pe baza acestor roluri;
- Solutia trebuie sa permita posibilitatea de a partaja date astfel incat utilizatorii pot primi acces la obiecte care nu le apartin pentru a realiza diferite sarcini colaborative;
- Solutia trebuie sa asigure prevenirea accesului la obiecte care nu apartin utilizatorului sau la care nu are acces prin partajare;
- Solutia trebuie sa ofere securitate la nivel de obiecte;
- Solutia trebuie sa asigure diferite niveluri de acces asupra obiectelor.

### 3. Cerinte specifice pentru managementul fluxurilor de lucru (workflow)

- Solutia trebuie sa permita definirea si publicarea de workflow-uri personalizate.
- Sa permita definirea unor template-uri de workflow
- Sa ofere in standardul aplicatiei functionalitatea de definire a workflow-urilor care sa fie rulate

manual sau automat in functie de un anumit eveniment (introducerea unei inregistrari, schimbarea statusului unei inregistrari, asignarea unei inregistrari, schimbarea valorii unui camp pe o inregistrare, stergerea unei inregistrari)
- Solutia trebuie sa ofere o interfata web de administrare a workflow-urilor.
- Workflow-urile rulate sau cele care vor fi rulate pe o inregistrare sunt vizibile utilizatorilor in interfata web pe inregistrarea in cauza.

## 3. Bază de date de tip enterprise

- Solutia trebuie sa ofere un suport implicit scalabil, disponibil si sigur pentru baze de date relationale, incluzand instrumente integrate de raportare si analiza, business intelligence, consolidare / integrare de date, masterizare si verificarea calitatii datelor, si Data Mining.
- De asemenea sistemul trebuie sa includa in mod nativ o platforma care sa permita procesarea complexa a evenimentelor, consistenta a datelor in medii heterogene, facilitati avansate pentru dezvoltare si servicii proprii de Business Intelligence (self-service BI). Solutia trebuie sa ofere urmatoarele functionalitati.

### 1. Cerințe de disponibilitate ridicată şi mentenanță :

- Posibilitatea de a crea solutii de disponibilitate ridicata fara sa fie necesare hard diskuri partajate (solutii tip SAN – Storage Area Network sau NAS – Network Attached Storage)
- Posibilitatea efectuarii backup-ului in multiple fisiere simultan pentru a putea efectua operatia pe discuri diferite in paralel.
- Posibilitatea efectuarii backup-ului direct intr-o solutie de cloud privat, respectand normele de securitate

### 2. Cerințe de raportare consolidata si managementul depozitelor de date:

- Index secundar la nivel de coloane care sa comprime si sa stocheze datele in memorie pentru access rapid la datele din Data Warehouse
- Posibilitatea de a procesa sute de milioane de linii in mai putin de o secunda pentru access rapid la rapoarte
- Afisarea rapoartelor intr-un mod interactiv, astfel incat utilizatorii sa poata urmari evolutia in timp a anumitor evenimente, sa poata efectua filtrari asupra datelor prezentate
- Depozit de date relational si instrumente OLAP: sistemul sa ofere in mod nativ solutii OLAP si data warehouse; data warehouse sa permita lucru in mod partitionat pentru incarcarea rapida si mentenanta usoara a tabelelor foarte mari
- ETL (Extract, transformation, load): functionalitati native de extragere a datelor din diferite surse de date (SQL Server, Oracle, Excel, Web services), realizarea de filtrari, agregari si diferite alte transformari asupra datelor si in final stocarea datelor in data warehouse.
- Baze de date multidimensionale native: stocarea datelor intr-un cub cu mai multe dimensiuni, in vederea interogarii mai usoare a datelor si construirii rapoartelor relevante.
- Posibilitati de raportare din surse de date cum ar fi: liste SQL Server, Oracle, SQL Server Analysis Services, SAP NetWeaver BI, Hyperion, Sharepoint List, Teradata, SQL Azure si SQL Server Parallel Data Warehouse , XML

- Posibilitati de raportare cu moduri multiple de vizualizari: harti, sparklines si indicatori.
    - Harti: Posibilitatea de creare de rapoarte folosind Map Wizard care permite vizualizarea datelor sub forma unui model geograficcare poate prelua datele dintr-o galerie de harti pe baza de interogari SQL sau dintr-un fisier stocat in sisteme tip ESRI. Elementele dintr-o harta pot fi poligoane (pentru reprezentare de arii), linii (pentru reprezentarea de rute si drumuri) si puncte (reprezentand locatii diverse). Se pot adauga date aditionale de afisare sau atentionari interactive folosind harti online.
    - Sparklines: Posibilitate de creare rapoarte folosind tabele si matrici pentru a afisa date agregate.
    - Indicatori: Posibilitatea de vizualizarea a datelor intr-un mod rapid folosind metode grafice (icoane).
- Instrumente de data mining: functionalitati pentru construirea de modele analitice complexe precum si integrarea acestor modele cu operatiile de business.
- Raportare “ad hoc”: utilizatorii sa poata edita propriile rapoarte pe baza unui model (template), fara sa detina cunostinte de baze de date sau despre structura acestora. Serviciile de raportare sa fie incluse in produs, fara add-on-uri suplimentare.
- Interogare si analiza ad-hoc si self-service a datelor: facilitati de interogare a datelor disparate in momentul solicitarii rapoartelor.
- Extragerea si editarea dinamica a rapoartelor utilizand instrumente familiare de tip Office (i.e. Microsoft Excel) si interfete noi intuitive si productive care includ harti, sparklines si indicatori.
- Posibilitati de colaborare cu ajutorul instrumentelor de analiza de tip pivot, accesibile via un browser web, care sa permita utilizatorilor sa creeze solutii self-service BI cu platforme portal de tip colaborativ pe seturi de date mari (mai mult de 1 milion de randuri pentru un fisier de maxim 2Gb dimensiune).

### 3. Cerințe de gestionare facila a obiectelor bazelor de date:

- Instrumente de dezvoltare a obiectelor din baza de date: solutia trebuie sa ofere unelte de dezvoltare pentru modulele ETL (Extract, Transform, Load), pentru design-ul bazelor de date atat relationale cat si multidimensionale, pentru design-ul rapoartelor.
- Unelte pentru administrarea bazelor de date si a proceselor uzuale care se executa asupra bazelor de date precum si al rapoartelor
- Posibilitatea de definire si gestionare a obiectelor bazei de date (tabele, indecsi, proceduri stocate, triggere) direct din instrumentele folosite de dezvoltatori pentru scrierea aplicatiilor
- Posibilitatea de a oferi compresia datelor folosind suport UCS-2 Unicode
- Loc central care ofera posibilitatea administrarii entitatilor de date si ierarhiilor din multiple baze de date cu posibilitatea versionarii

### 4. Cerințe de performanță ridicată a sistemului de baze de date:

- Criptarea transparenta a datelor, a fişierelor de date şi a fişierelor jurnal fără să fie necesară modificarea aplicației. Functionalitatile de criptare sunt necesare pentru indeplinirea cerințelor şi respectarea reglementărilor generale cu privire la confidențialitatea datelor. Criptarea trebuie sa ofereinclusiv instrumente de căutare in datele criptate utilizând sisteme de regasire într-un interval sau căutarea parțială, fără modificarea aplicațiilor existente.

- Auditarea operatiilor: auditarea trebuie sa includa informații despre momentul în care au fost citite datele, în plus față de orice modificare a datelor. Produsul trebuie sa ofere caracteristici precum configurarea îmbunătățită şi managementul auditurilor în server. Produsulsa defineasca specificațiile de audit în fiecare bază de date, astfel încât configurația auditului să poată fi adaptată pentru diversele baze de date.
- Posibilitatea de a filtra evenimentele auditate; posibilitatea de a customiza operatia de audit in functie de evenimentele pentrecute in baza de date
- Posibilitatea adăugarii online a resurselor de memorie la masinile fizice care gazduiesc bazele de date, pentru scalarea la cerere a acestora.
- Colectarea datelor de performanță: facilitati de optimizare şi depanare a performanței server-ului de baze de date, pentru a furniza administratorilor o perspectivă interactivă cu privire la performanță
- Sistem de monitorizare extins al evenimentelor: sistem general de tratare a evenimentelor la nivel de serverprin captarea, filtrarea şi reglarea evenimentelor generate de procesele de server. Evenimentele trebuie sa poata fi captatesi exportate in diferite formate de ieşire, inclusiv Event Tracing for Windows (ETW), pentru corelarea cu aplicațiile sistemului de operare şi ale bazelor de date, permițând astfel o monitorizare completă a sistemului.
- Factorul de compresie al backup-urilor trebuie sa fie minim 60%
- Posibilitatea definirii limitelor şi priorităților resurselor pentru diferite sarcini (workloads), si obtinerea unei performanțe consecvente in executarea acestora. Modul de alocare a resurselor fizice ale server-ului trebuie sa poata fi controlat de catre administratorul de sistem. Sistemul trebuie sa ofere stabilitate şi predictibilitate sporită asupra performanțelor de interogare, furnizând funcționalitati pentru blocarea planurilor de interogare, permițând organizației să promoveze planuri stabile de interogare în timpul înlocuirii hardware-ului serverului, în timpul upgrade-urilor serverului şi în timpul instalărilor instanțelor de producție.
- Asigurarea continuitatii activitatii organizatiei: duplicarea datelor prin tehnologii de tip data mirorring
- Livrarea automata a log-urilor bazei de date catre Data Recovery Center

### 5. Cerințe de implementare a structurilor de date complexe:

- Posibilitatea nativa de modelare a structurilor de date de tip arbore: metode încorporate pentru crearea şi operarea pe noduri ierarhice.
- Posibilitatea stocarii datelor binare mari, precum documente şi imagini, ca parte integranta a bazei de date, păstrand in acelasi timp consecvența tranzacțională.
- Căutare complexa la nivel de text, folosindindecsi specializati; efectuarea rapida a căutărilor in acest tip de date
- Managementul performant al coloanelorcu valori rare: modalitati eficiente pentru administrarea spatiilornecompletate dintr-o bază de date relationala, astfel incat valorile de tip NULL să nu consume spațiu fizic.
- Posibilitatea crearii de tabele cu mai mult de 1.024 de coloane.

### 6. Alte cerințe

- Platforma de gestiune a bazelor de date trebuie să permita utilizarea unei platforme avansate pentru dezvoltarea de aplicatii complexe de procesare a evenimentelor (CEP). Acest lucru trebuie să ofere
    - Posibilitatea de dezvoltarea de aplicatii bazate pe evenimente folosind platforma de

procesare a evenimentelor pentru a se permite interogari continue si latenta de milisecunde.

- Posibilitatea de dezvoltare de aplicatii care sa creasca valoarea de business prin scaderea costului de extragere, analiza si corelare a datelor permitand monitorizarea si managementul datelor in timp real.
- Costuri totale de detinere. Sistemul trebuie sa ofere mecanisme pentru reducerea costului total de detinere (TCO), si prin implementarea administrarii bazate pe politici pentru:
    - Definirea si managementul politicilor de configurare a sistemului
    - Monitorizarea şi prevenirea modificarilorasupra sistemului prin crearea de politici împotriva configurării
    - Detectarea problemelor de conformitate cu politicile direct din interfata de administrare a server-ului
    - Posibilitati de virtualizare pentru a creste ROI (Return On Investment) prin consolidare si virtualizare

## 4. Software virtualizare și management servere

Platforma de virtualizare tip server trebuie sa indeplineasca urmatoarele cerinte specifice:

- Platforma de virtualizare trebuie sa fie bazata pe Hypervizor propriu, fara dependenta de un sistem de operare anume.
- Hypervizorul sa fie independent de metoda de stocare interna/externa a serverului/serverelor pe care ruleaza.
- Platforma de virtualizare sa fie compatibila si recunoscuta de majoritatea producatorilor hardware consacrati:
    - IBM,
    - Dell,
    - HP,
    - Sun,
    - Intel.
    - etc
- Administrarea platformei virtuale sa se poata face atat prin consola locala /la distanta cat si prin browser web si prin platforma de management dedicata.
- Sa aiba suport pentru urmatoarele sisteme de operare :
    - Windows XP/Vista/7/2003/2008/2008 R2,
    - Linux Suse/Red Hat/CentOS,
    - FreeBSD,
    - Solaris,
    - Netware.
- Sa se poata adauga cu usurinta spatiu de stocare pentru masinile virtuale prin folosirea a cel putin urmatoarelor protocoale :
    - NAS – NFS/CIFS ;
    - SAN – iSCSI/FCP.
- Sa se poata adauga cu usurinta spatiu de stocare pentru masinile virtuale prin folosirea a cel putin urmatoarelor sisteme de fisiere :
    - FAT32,
    - NTFS,
    - EXT2,
    - EXT3.

- Componentele platformei hardware virtuale prezentate sistemelor de operare din masina virtuala sa poata fi modificate cu usurinta ( adaugare/eliminare ).
- Sa suporte adaugarea de resurse de procesare si memorie fara repornirea sistemului de operare din masina virtuala.
- Hypervizorul si platforma de management a infrastructurii virtuale sa fie de la acelasi producator.
- Platforma de virtualizare sa permita independent sau prin conectori/componente proprietare/terte virtualizarea componentelor de procesare, retea si stocare.
- Sa permita configurarea retelei virtuale prin integrarea directa cu platforma de retea aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de retea.
- Reteaua virtuala a platformei sa fie unificata la nivelul intregii infrastructuri virtuale, indiferent de numarul de servere ce fac parte din aceasta infrastructura.
- Reteaua virtuala sa fie configurabila la nivelul intregii infrastructuri virtuale si nu prin configurarea individuala a fiecarui server in parte.
- Sa permita agregarea conexiunilor fizice de retea precum si distribuirea incarcarii pe aceste conexiuni indiferent de producatorul serverelor si/sau placilor de retea folosite.
- Sa ofere redundanta la nivelul conexiunilor de retea fizice/virtuale indiferent de producatorul serverelor si/sau placilor de retea folosite.
- 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.
- Sa permita extinderea discurilor virtuale fara a fi necesara oprirea masinilor virtuale ce au atasate aceste discuri, daca sistemul de operare permite aceasta operatiune.
- Sa permita balansarea dinamica automata/manuala a resurselor de procesare existente in platforma virtuala in functie de necesitati si/sau pe baza unor reguli/politici prestabilite.
- Sa permita distribuirea dinamica si/sau manuala a masinilor virtuale in functie de gradul de ocuparea a resurselor de procesare.
- Sa permita gruparea si organizarea logica a resurselor de procesare in functie de necesitati.
- Platforma de virtualizare sa permita izolarea acestor grupari de resurse dar in acelasi timp sa fie suficient de flexibila incat sa se poata mari cantitatea de resurse disponibile intr-o grupare prin extragerea de resurse din alte grupari.
- Sa permita crearea de politici dinamice de acces la resursele de procesare, precum si de disponibilitate ale acestora.
- Pentru administrarea platformei de virtualizare sa permita autentificarea utilizatorilor prin intermediul unui sistem de tip director (LDAP, Kerberos sau similar) sau local.
- Sa permita separarea privilegiilor administrative in functie de roluri predefinite sau roluri configurabile manual.
- Separarea privilegiilor administrative sa se poata face pe orice element disponibil in interfata de administrare (server, utilizator, resursa de procesare, stocare, retea, etc).
- Sa permita crearea de zone/domenii de securitate in functie de aplicatii si/sau roluri functionale, nu numai in functie de server/servere.
- Separarea zonelor de securitate si a rolurilor administrative sa se faca integrat din platforma de management a infrastructurii virtuale.
- Din platforma de management sa se poata defini si aplica profile de configuratie standard pentru serverele ce fac parte din infrastructura virtuala. De asemenea sa permita configurarea de politici de aplicare a acestor profile in functie de necesitatile de moment sau in concordanta cu politica stabilita in prealabil.
- Sa permita integrarea prin intermediul unor conectori/componente cu platforma de stocare in vederea realizarii backup-ului direct din platforma de stocare.

- Sa asigure concomitent suport de pana la 8 procesoare logice si maxim 256 GB ram pentru oricare maşină virtuala, daca sistemul de operare din masina virtuala poate adresa aceasta cantitate de resurse de procesare.
- Sa permita mutarea 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.
- Sa permita mutarea intregului hard-disk 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.
- Sa permita extinderea automata a harddisk-urilor virtuale pe masura ce sistemul de operare si aplicatiile din masinile virtuale o cer.
- Sa permita in mod automat, prin politice predefinite, consolidarea masinilor virtuale pe un numar prestabilit de servere si sa opreasca automat serverele fara activitate sau cu subutilizare a resurselor de procesare.
- 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 oferi licentele de utilizare a platformei de virtualizare tip server pentru toate procesoarele fizice si logice oferite.

## 5. Software mesagerie electronică

Soluția software de mesagerie electronica ofertată trebuie să îndeplinească  următoarele cerințe:

**Usurinta in utilizare:**

- Solutia sa ofere asistenta vizuala pentru alegerea celor mai bune date si ore pentru intalniri, in functie de programul invitatilor si resurse.
- Posibilitatea de a vedea informatiile despre disponibilitatea persoanelor din calendar.
- Salile de conferintasi echipamentele sa fie marcate clar in agenda, astfel incat sa poata fi parcurse separat.
- Sa se poata programa mesaje ‘‘Out-of-Office’’ separate, pentru a fi trimise unor destinatari interni sau externi dupa preferinta mesaje diferite.
- In cazul accesului la casuta postala prin Web sa se permita convertirea documentelor (ex. Microsoft Office Word, Excel®, PowerPoint® şi PDF) astfel incat sa poata fi vizualizate chiar daca aplicatiile respective nu sunt instalate pe calculatorul client. Deasemenea, accesul prin Web sa aduca functionalitati extinse gen schedule assistant, categorii de mesaje, cautari avansate
- Lucru colaborativ facil din interfata Web, adica daca un utilizator primeste o legatura la un document de pe un sistem de partajare a fisierelor, sistemul de mesagerie sa preia linkul si sa faca cererea in numele utilizatorului pentru a afisa documentul.

- Accesul la casutele postale sa se poata face si de pe dispozitive mobile. Mai mult, daca un dispozitiv este pierdut sau furat, utilizatorul sa poata sterge remote continutul dispozitivului mobil sau sa poata reseta parola prin interfata Web.

- Usurinta in realizare de reguli pentru a redirecta corespondenta in diverse arhive, containere sau destinatii,

- Posibilitatea de a marca corespondenta cu diferite culori in functie de importanta, pentru o vizibilitate mai buna.

- Posibilitatea de a grupa e-mailurile in functie de topic, destinatar, identificator etc.

- Informatii oferite in legatura cu destinatiile din interiorul institutiei catre care dorim sa trimitem corespondenta (exemplu: daca persoana respectia este in concediu; daca in componenta grupului catre care dorim sa trimitem un mesaj exista si oameni din afara institutiei etc)

**Eficienta in administrare si securitate**

- Sistemul de mesagerie trebuie sa asigure performante ridicate si fiabilitate, pe masura ce cresc dimensiunile casutelor postale si numarul de conturi de utilizator per server. Sa aiba capacitatea sa acomodeze cantitati foarte mari de mesaje la performante ridicate.

- Sistemul sa ofere un grad ridicat de securitate, care sa poate fi integrat nativ cu PKI (infractrucura de chei publice) sau cu RMS (sistem de gestionare a drepturilor de acces la informatie) usor de folosit si integrat nativ cu o soluție LDAP (Ex Microsoft Active Directory).

- Platforma trebuie sa fie extensibila pentru servicii web pentru a le putea permite dezvoltatorilor sa integreze informatii din casutele postale sau calendar cu aplicatii specifice companiei sau alte aplicatii personalizate.

- Sistemul sa permita filtrarea antispam disponibila de la instalare, fiind gestionata de rolul de server Edge Transport, in perimetrul retelei si sa ofere un mecanism de protectie impotriva virusilor si al viermilor de retea.

- Arhitectura sa asigure o inalta disponibilitate si replicarea bazelor de date cu casutele postale. Baza de date sa poata sa fie replicata si pe alte servere de mesagerie din institutie, si in cazul in care baza de date primara este corupta, automat utiliatorul sa fie redirectat catre alta copie a casutei postale.

- E-mailurile din interiorul organizatiei sa fie criptate automat, de la plecarea din clientul de e-mail al expeditorului, pana la primirea în clientul de e-mail al destinatarului.

- Configurarea aplicatiei client de e-mail,in vederea conectarii la server, sa se faca usor, de genul ca daca utilizatorul este conectat la retea, serverul de mesagerie prin componentele sale sa configureaze automat profilul de email al utilizatorului.

- Pentru a putea impune anumite reguli (interne, guvernamentale sau locale) sistemul trebuie sa fie capabil, prin control detaliat asupra fluxurilor de e-mailuri,saimplementeze un motor pentru politici.

- Pentru a asigura certificarea mesajelor administratorii trebuie sa poata utiliza reguli de transport pentru a aplica clasificari ale mesajelor pentru e-mailurile in tranzit, in functie de subiect, continut sau adresa expeditorului/destinatarului. Sa existe posibilitatea folosirii unui proces automat care sa scaneze foldere predefinite de administrator pentru a retine, expira sau jurnaliza mesajele, in functie de normele care trebuie respectate.

- Sistemul sa poata permite realizarea de cautari text rapide in cadrul tuturor casutelor postale din organizatie, daca este necesara această actiune din punct de vedere legal.

- Sistemul de mesagerie sa permita integrarea cu centrala telefonica existenta pentru a adauga functionalitati de cutie vocala cat si IVR (recunoasterea inteligenta a vocii) pentru utilizatorii din institutie.

- Produsul sa ofere sistemului de operare contorii necesari pentru a putea fi urmarita starea de functionare si performanta in fiecare clipa cat si integrarea cu diferite unelte de monitorizare.

- Consolele de aministrare sa fie intuitive si usor de utilizat.

- Sistemul sa poata delega drepturi diferite pentru anumite departamente sau grupuri de persoane pentru a asigura segregarea drepturilor in functie de responsabilitatile fiecarui utilizator.

- Sistemul sa dispuna de unelte care sa permita rularea de comenzi text cat si realizarea facila de scripturi pentru a automatiza diverse actiuni cat si pentru a automatiza instalarea aplicatiei pe o platforma noua.

- Sistemul sa ofere interfata de autoadministrare pentru utilizatori.

- Sistemul sa ofere protocoale de acces la casuta postala: POP, IMAP, WEB plus protocolul MAPI pentru integrare cu Microsoft Outlook.

- Sistemul sa ofere unelte de jurnalizare si arhivare la nivel global sau pentru un numar restrans de utilizatori, sa afere capabilitate utilizatorului sa isi arhiveze singur e-mailurile.

- Sistemul sa ofere interfata de autoadministrare pentru utilizatori, astfel incat utilizatorii sa poata realiza urmatoarele sarcini pentru gestiunea casutei postale: resetare parola, reguli de gestiune a mesajelor, sa schimbe apartenenta la grupuri de distributie, sa poata face cereri de a deveni membru la grupuri de distributie, setare Out-of-office cu customizare mesaj de auto-raspuns, sa poata obtine rapoarte de livrare mesaje dupa diverse criterii, posibilitatea de a seta limba pentru interfata de utilizare (Romana sau alte limbi),

## 6. Sisteme de operare și securitate client

### 1. Platforma de virtualizare desktop

Soluția trebuie să ofere utilizatorilor un desktop virtual, pe care să îl poată accesa de pe un calculator fizic conectat la rețeaua internă. Acest desktop virtual va folosi resursele serverului și nu ale stațiilor locale.

Oferta va include în preț servicii de consultanță tehnică prin specialişti ai Ofertantului şi specialişti ai producătorului. Se solicită ca implicarea specialiștilor ceritifcați de producător să fie în toate etapele de derulare după cum urmează:

- Analiză;
- Elaborare arhitectură soluție;
- Implementare și configurare;
- Testare și stabilizare;
- Elaborare documentație și transfer de cunoștințe către persoanele desemnate din partea beneficiarului.

a) Cerințe generale

- Adăugarea rapidă de aplicații și desktop-uri noi, disponibile imediat tuturor utilizatorilor;
- Folosirea inteligentă a resurselor hardware;
- Reducerea efortului de management al administratorilor și scăderea timpului de răspuns în cazul unei probleme a utilizatorilor;
- Minimizarea resurselor hardware, micșorând astfel consumul de energie electrică;
- Crearea unui mediu scalabil care poate răspunde cerințelor în mod dinamic și automatizat.
- Să ofere utilizatorilor acces la desktopul virtual, folosind oricare calculator conectat la rețeaua internă;
- Să minimizeze efortul administrativ în cazul în care se dorește modificarea imaginilor desktop;
- Să ofere o singură consolă de administrare a întregii infrastructuri VDI;

- Să permită crearea de mașini noi, cu un efort minim din partea administratorilor;
- Să permită folosirea unei singure imagini de tip “master” care sa fie replicată într-un număr suficient de mașini virtuale, având aceleași caracteristici.
- Să ofere utilizatorilor acces la toate aplicațiile folosite în mod curent;
- Să permită instalarea update-urilor și a aplicațiilor fără a întrerupe accesul utilizatorilor;
- Să ofere scalabilitate sistemului și să permită adăugarea de noi resurse hardware, pentru a acomoda un număr mai mare de utilizatori;
- Să permită restaurarea, în caz de incident, a imaginii fidele a fiecărei stații de lucru într-un timp cât mai scurt;
- Funcționare în medii LAN;
- Să fie compatibilă cu sisteme de virtualizare de server de tip Hyper-V
- Suport pentru rularea în desktopurile virtuale a sistemelor client Windows 7 si Windows 8 pe arhitecturi de 32 și 64 de biți;
- Să ofere posibilitatea accesării desktopurilor virtuale prin protocol de tip Remote Desktop (RDP)
- Desktopurile virtuale să folosească virtual placa grafică a hostului de virtualizare pentru rularea de aplicații multimedia audio și video (vGPU); daca placa grafica nu suport DirectX 11, sistemul trebuie sa emuleze un GPU (software softGPU).
- Să ofere managementul update-urilor și patchurilor pentru desktopurile virtuale
- Să ofere optimizarea lățimii de bandă si suport pentru TCP si UDP
- Să ofere managementul profilelor utilizatorilor;
- Sa ofere suport pentru multi-touch
- Sa ofere suport pentru Single Sign-On

b) Cerinte functionale pentru solutia de virtualizare a sesiunilor

Solutia trebuie sa permita rularea aplicatiilor pe server si sa trimita doar ecranul aplicatiei pe statia utilizatorului. Prin aceasta solutie, se urmareste maximizarea utilizarii resurselor hardware, asigurand un nivel inalt de flexibilitate si scalabilitate intregului sistem.

Din punct de vedere al experientei utilizatorului, aplicatia se va vedea intr-o simpla fereastra, ca si cum ar rula pe echipamentul de calcul local.

c) Solutia de virtualizare trebuie sa ofere urmatoarele functionalitati:

- Sa permita utilizarea resurselor serverului, pentru a livra utilizatorului fereastra aplicatiei, la nivelul echipamentului de calcul local. Aplicatia sa ruleze pe server in timp ce utilizatorul acceseaza doar fereastra respectiv aplicatii, folosind desktopul personal.
- Sa permita acomodarea unui numar mare de utilizatori. In cazul in care cererea va creste, sa

permita cresterea numarului de utilizatori suportati prin adaugarea de noi resure de server

- Sa permita folosirea tehnologiilor de Application Virtualization pentru a elimina dependintele legate de sistemul de operare

d) Beneficii urmarite prin implementarea solutiei:

- Adaugarea rapida de aplicatii noi, disponibile imediat tuturor utilizatorilor
- Folosirea inteligenta a resurselor hardware
- Minimizarea resurselor hardware idle, micsorand astfel consumul de energie electrica
- Crearea unui mediu scalabil care poate raspunde cerintelor in mod dinamic si automatizat

e) Cerinte functionale pentru solutia de virtualizare a setarilor utilizatorului.

Solutia trebuie sa permita utilizatorilor sa aiba o experienta consistenta, indiferent de echipamentul de calcul de pe care se logheaza sau masina virtuala folosita.

- Sa stocheze si salveze setarile utilizatorilor legate de aplicatiile Office si cele din sistemul de operare
- Sa ofere utilizatorilor acces la setarile personale, cand acceaza orice statie client din domeniu
- Sa permita redirectarea folderelor importante pentru utilizator (My Documents, Desktop, etc) catre un FileServer unde acestea pot fi salvate si protejate.

#### 2. Sistem de operare tip desktop

Toate stațiile de lucru din cadrul acestui proiect vor fi livrate cu minim sistem de operare tip Windows 7 Professional OEM sau echivalent.

Se vor oferi licentele de utilizare a platformei software tip sistem de operare desktop pentru 45 utilizatori interni ai Sistemului

## 7. Sisteme de operare server

#### 1. Sistem de operare pentru platformele tip portal si componenta colaborativa tip CRM

Sistemele de operare ce se va instala pe echipamentele hardware tip server trebuie sa indeplineasca urmatoarele cerinte:

- Sa ofere suport pentru minim 2 socketuri procesor;
- Sa ofere suport pentru urmatoarele tipuri de procesoare:
  - x86;
  - x86-64;
- Sa ofere suport pentru tehnologia 64-bit;
- Sa ofere suport pentru urmatoarele tipuri de conectivitate cu echipamentele de stocare :
  - NAS;
  - SATA;

    - SAS;
    - SCS;
    - FC;
    - FcoE;
    - iSCSI.
- Sa permita instalarea in configuratii cluster tip “high-availability”;
- Sa ofere suport pentru tehnologia de “virtualizare” (virtualizarea nodurilor de procesare, vezi cap 3.2.3.6 – “Licenta software virtualizare si management server-e”);
- Sa ofere o interfata unica pentru configurarea si monitorizarea serverului;
- Sa ofere o componenta shell cu linie de comanda si limbaj de script;
- Sa ofere instrumente de diagnosticare asupra mediului serverului, fizic si virtual;
- Sa permita administrarea serverului de la locatii de la distanta;
- Sa permita instalari in configuratie minimala;
- Sa includa mecanisme de “backup” a datelor.

Se vor oferi licentele de utilizare a sistemelor de operare dimensionate dupa necesitati, dar nu mai putin de 30 de instante virtualizate care sa ruleze distribuite pe  serverele fizice.

**2. Sistem de operare pentru componenta front-end web**

Sistemele de operare ce se vor instala pentru componenta front-end web trebuie sa indeplineasca urmatoarele cerinte:

- Sa ofere suport pentru minim 2 socketuri procesor;
- Sa ofere suport pentru urmatoarele tipuri de arhitecturi de procesoare:
    - x86, x86_64;
    - POWER sau echivalent;
- Sa ofere suport pentru tehnologia 64-bit;
- In arhitecturi  tip x86_64 sa fie testat si certificat de producator ca poate gestiona cel putin 1TB de memorie si cel putin 160 de procesoare
- Sa ofere suport pentru fisiere de dimensiuni mari: peste 8TB filesize
- Sa ofere suport pentru urmatoarele tipuri de conectivitate cu echipamentele de stocare :
    - NAS;
    - SATA;
    - SAS;
    - SCS;
    - FC;
    - FcoE;
    - iSCSI.
- Sa permita instalarea in configuratii cluster tip “high-availability”  si load-balance;
- Sa ofere suport pentru tehnologia de “virtualizare” (virtualizarea nodurilor de procesare, vezi cap 3.2.3.6 – “Licenta s