APROB
PRESEDINTE
Delia POPESCU

Caiet de sarcini SICAP
Sistem informatic colaborativ pentru achizitii publice

1. DATA GENERALE

1.1 Denumirea proiectului

„Sistem informatic colaborativ pentru achizitii publice”- **SICAP.**
Beneficiarul si entitatea resonsabila cu implementarea proiectului este Agentia pentru Agenda Digitala a Romaniei.
Toate cerintele prezente in acest document sunt minime si obligatorii. Ofertantul va include in solutie toate elementele solicitate, respectiv toate elementele necesare bunei functionarii a solutiei propuse in confomritate cu arhitectura si considerenele de proiectare alese de catre acesta.

1.2 Amplasamentul

Toate livrabilele proiectului vor fi livrate si instalate la sediul Agentiei pentru Agenda Digitala a Romaniei, Str. Italiană nr.22, sector 2, Bucureşti, România.
Echipamentele/produsele livrate, vor fi noi şi in cea mai recenta versiune, de fabricaţie curenta si vor fi comandate pentru Beneficiar.
Toate costurile de import, asigurare, manipulare, transport si instalare in toate locaţia proiectului vor fi asigurate de catre ofertant.

2. SCOPUL SI OBIECTIVELE PROIECTULUI

Obiectivul proiectului propus constă în dezvoltarea unui mediu performat de desfasurare a achizitilor publice in linie cu cerintele Uniunii Europene si cu legislatia in vigoare privind achizitiile publice. Proiectul asigurara cresterea eficienţei serviciilor publice prin oferirea serviciilor administrative folosind mijloace electronice moderne, eficiente, eficace şi accesibile, bazate pe paradigme de interoperabilitate, siguranţă şi trasabilitate, în vederea creării de beneficii pentru cetăţeni, persoane juridice şi pentru administraţia publică.
Obiectivul general al proiectului va fi atins cu ajutorul următoarelor obiective specifice:

- Asigurarea unui mediu concurential si competitiv pentru accesul la fondurile publice prin implementarea unui portal de gestionare a achizitiilor;
- Eficientizarea activităților pentru toate entitățile implicate prin asigurarea unui platforme de lucru colaborativ;
- Cresterea gradului de transparenta a proceselor de achizitii publice prin utilizarea de standarde deschise;
- Asigurarea unui grad ridicat de securitate si de protectie a informatiilor ce apartin instutiilor publice si private prin utilizarea unei infrastructuri cu chei publice;
- Îmbunătăţirea eficienţei profesionale a angajaţilor prin asigurarea accesului rapid la informaţiile necesare îndeplinirii sarcinilor şi atribuţiilor;
- Reducerea costurilor administrative şi a timpilor de răspuns la solicitările cetăţenilor.

Atingerea obiectivelor menţionate va fi posibilă prin implementarea Sistem Informatic Colaborativ pentru mediu performat de desfasurare al Achizitiilor Publice – SICAP.

3. CERINTE FUNCTIONALE SI TEHNICE

3.1 Cerinte generale

Ofertantii vor trebui sa asigure migrarea datelor din sistemul existent SEAP (proceduri inchise si in desfasurare, entitati, documente atasate procedurilor) si integrarea lor functionala in structura si arhitectura noului sistem. Structura bazei de date si arhitectura sistemului va fi pusa in faza de analiza la dispozitia ofertantului declarat castigator. De asemenea, tranzitia la noul sistem trebuie sa se faca transparent pentru utilizatorii finali fara a avea impact asupra sistemului public de achizitii, in special fara intreruperea functionarii acestuia. Ofertantul va detalia in cadrul solutiei propuse strategia si modalitatea aleasa pentru migrarea datelor si asigurarea functionarii permanente a serviciilor sistemului public de achizitii.

3.2 Cerinte functionale ce trebuiesc indeplinite de sistemul SICAP

Sistemul implementat trebuie sa respecte cadrul legislativ privind achizitiile publice, repectiv, dar nelimitat la:

- ORDONANŢA DE URGENŢĂ Nr. 34/2006 privind atribuirea contractelor de achiziţie publică, a contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii – ca lege de bază privind achiziţiile publice;

- HOTĂRÂREA GUVERNULUI Nr. 925/2006 pentru aprobarea normelor de aplicare a prevederilor referitoare la atribuirea contractelor de achiziţie publică din OUG 34/2006 – ca legislaţie secundară;
- HOTĂRÂREA GUVERNULUI Nr. 71/2007 pentru aprobarea normelor de aplicare a prevederilor referitoare la atribuirea contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii prevăzute de OUG 34/2006 – ca legislaţie secundară(imediat după aderare);
- Ordine ale Preşedintelui A.N.R.M.A.P.– ca legislaţie terţiară;
- "Manual operaţional pentru atribuirea contractelor de achiziţie publică"
- Single Market Act emis de Comisia Europeană în decembrie 2011 (IP/11/1580)
- Norme de functionare UCVAP

Serviciile descrise mai jos trebuie sa respecte prevederile legislatiei privind achizitiile publice.

3.2.1 Servicii pentru autoritatile contractante

Serviciul profil autoritati contractante

Serviciul profil autoritate contractanta trebuie sa permita utilizatorilor accesul la urmatoarele categorii de informatii:

- elementele de identificare ale entităţii: nume, cod de identificare fiscală, număr de înrergistrare la registrul comerţului, reprezerntantul legal, banca şi contul bancar
- tipul de entitate, şi anume dacă prestează în domeniul utilităţilor sau nu, care este tipul de activitate în care se încadrează, dacă este ordonator de credite principlal, secundar sau terţiar, şi dacă se subordonează vreunei alte autorităţi contractante şi dacă da, care este aceasta;
- adresele folosite de entitate trebuie sa contina informatiile uzuale pentru o adresa (stradă, număr, persoană de contact etc.); trebuie sa existe minim o adresa de contact;
- un set de documente de referinţă
- entităţile subordonate, dacă există
- lista utilizatorilor unei entitati si rolurile asociate acestora

Serviciul Anunturi de intentie si Invitatii de participare

Acest serviciu trebuie sa asigure autoritatilor contractante posibilitatea publicarii in sistem a anunturilor de intentie si a invitatiilor de participare pentru procedurile pe care intentioneaza sa le desfasoare in viitor (pentru contractele de achizitie a caror valoare estimata depaseste un anumit prag stabilit prin lege, o autoritate contractanta este obligata sa publice un anunt de intentie).

Trebuie sa se permita definirea un singur anunt de intentie pentru mai multe proceduri, sau un anunt pentru o singura procedura.

Formularele care stau la baza definitii anuntului respectiv invitatiei trebuie sa respecte legislatia in vigoare.

Anunţul de intenţie trebuie sa poata fi defalcat în funcţie de tipul contractului, adică fie lucrări, fie furnizări şi servicii, şi în funcţie de legislaţie, în domeniul apărării şi securităţii sau nu. De asemenea, trebuie permisă desemnarea anunţul de intenţie ca fiind de utilităţi sau non-utilităţi. Autoritatea contractantă trebuie sa poata defini în cadrul anunţului de intenţie o serie de loturi, dacă este cazul. Publicarea unui anunţ de intenţie trebuie sa se realizeze dupa validarea acestuia de catre ANRMAP.

Odată publicat, un anunţ de intenţie trebuie sa poata fi asociat unui anunţ de participare aflat în definire.

Serviciul Cereri de oferta

Acest serviciu trebuie sa ofere posibilitatea autoritatilor contractante sa initieze cereri de oferta prin intermediul sistemului si sa completeze informatiile aferente acestora.

Pentru achizitiile pe baza de cerere de oferta AC-urile trebuie sa poata defini in sistem invitatii de participare. O cerere de oferta se poate desfasura online prin sistem sau offline. In ambele cazuri trebuie completata o invitatia de participare la initierea achizitiei.

In cazul in care procedura se desfasoara offline, AC-ul trebuie sa poata completa un formular care trebuie sa contina cel putin informatiile prevazute in lege.

Informatiile continute in invitatia de participare trebuie sa fie:

- data limita de depunere oferta;
- adresa la care se transmit ofertele;
- limba sau limbile in care se redacteaza;
- criterii minime de calificare;
- descrierea obiectului contractului;
- modul de obtinere a documentatiei;

AC-ul trebuie sa poata atasa documentaţia de atribuire la invitatia de participare, sub forma unor fisiere uploadate. Deasemenea dupa publicarea acesteia, AC-ul trebuie sa poata formula clarificari sub forma de documente (fisiere uploadate in sistem) sau prin completarea unui comentariu sub forma de free text.
Serviciul trebuie sa ofere un mecanism de departajare a ofertelor utilizand unul dintre urmatoarele criterii: "pretul cel mai scazut" sau "cea mai avantajoasa oferta economica".
Sistemul trebuie sa permita criptarea ofertei de prêt la depunere.
Sistemul trebuie sa ofere urmatorul mecanism de defasurare al procedurii: Iniţial, pentru cererile de ofertă online ofertanţii se înscriu la procedură, consumînd astfel o participare preplătită, şi depun ofertele financiare şi-sau răspunsurile la criteriile de evaluare, acolo unde este cazul. Autoritatea contractantă evaluează apoi din punct de vedere tehnic şi apoi financiar aceste oferte, marcînd participanţii ca admişi sau respinşi, desermnînd în final un cîştigător şi atribuind procedura.

Serviciul Produse de catalog

Acest serviciu trebuie sa ofere posibilitatea ofertantilor de a publica un catalog de produse / servicii / lucrari si de asemena trebuie sa ofere autoritatilor contractante posibilitatea sa cumpere produse / servicii / lucrari prin alegerea unui produs / serviciu / lucrare din catalogul ofertantilor.
Acest serviciu trebuie sa ofere fiecarui operator economic posibilitatea de a-si gestiona propriul catalog cuprinzand produse, servicii si lucrari. Se poate defini in catalog produse, servicii si lucrari doar pentru toate codurile CPV publicate pentru procedura de cumparare directa.
Definirea produsului, serviciului sau lucrarii din catalog trebuie sa presupuna completarea minim a urmatoarelor elemente:

- denumire;
- cod produs, serviciu sau lucrare (unic la nivel de ofertant);
- codul CPV;
- descriere;
- pret de catalog;

Doar produsele publicate trebuie sa fie vizibile autoritatilor contractante (AC) si pot constitui obiectul achizitiei prin cumparare directa.
Numărul de produs / serviciu / lucrare disponibil pentru afişare trebuie sa fie limitat de numărul de poziţii cumpărate de respectivul ofertant.

Serviciul Cumparari directe

Acest serviciu trebuie sa asigure autoritatilor contractante desfasurarea cumpararilor directe prin intermediul sistemului. Sistemul trebuie sa permita desfasurarea procedurii prin efectuarea urmatoarelor etape:
Initiere achizitie - AC-ul consulta cataloagele ofertantilor, alege un produs, serviciu sau lucrare, completeaza conditiile de livrare si plata, cantitatea, unitatea de masura si optional pretul maximal. Deasemenea va stabili si data limita pana la care ofertantul poate formula raspunsul.
Decizie ofertant - la primirea cererii, ofertantul are doua optiuni:

- sa refuze cererea AC-ului, caz in care e obligat sa completeze motivatia refuzului;
- sa accepte cererea AC-ului, caz in care va completa valorile pentru cheltuielile suplimentare si discount; completarea acestor campuri este optionala; pretul final se va calcula adunand la pretul de catalog valoarea cheltuielilor suplimentare si scazand valoarea discountului;

In cazul in care ofertantul nu furnizeaza nici un raspuns pana la data limita stabilita de AC, procesul de achizitie se va inchide, iar licitatia nu se va mai atribui.
Decizie AC (etapa apare doar daca ofertantul a acceptat cererea in faza anterioara) - la primirea ofertei AC-ul are doua posibilitati:

- sa accepte oferta operatorului economic;
- sa refuze oferta, caz in care va completa motivul refuzului.

Serviciul de Licitaţie deschisă

Acest serviciu trebuie sa ofere posibilitatea autoritatilor contractante sa desfasoare proceduri de tip licitatie deschisa prin intermediul sistemului.
Serviciul de licitaţie deschisă trebuie sa permita, atît în cazul anunţurilor de participare cît şi a invitaţiilor de participare, consemnarea în cadrul sistemului a tuturor operaţiunilor care se desfăşoară, din punct de vedere al ofertelor financiare, al documentaţiei care trebuie ataşată, sau a răspunsurilor ofertanşilor la diferitele cerinţe ale autorităţii contractante. Licitaţia deschisă desfăşurată online trebuie sa fie împărţită în etape eşalonate secvenţial.
În funcţie de valoarea estimată, procedura trebuie sa treaca prin etapa de validare ANRMAP şi prin etapa de publicare la OJEU.
Desfasurarea licitatiei deschise trebuie sa contina urmatoarele etape:

- Prima etapă este cea de creare a licitaţiei deschise, în care autoritatea contractantă defineşte cerinţele licitaţiei deschise, avînd de ales între criteriul preţ şi oferta tehnică cea mai avantajoasă, în acest din urmă caz trebuind să specifice şi criteriile tehnico-economice ce vor intra în evaluare, ele putînd de asemenea fi criterii direct proporţionale (o valoare mai mare este mai bună) sau invers proporţionale (o valoare mai mică este mai bună). În funcţie de prezenţa sau nu a unei faze finale de licitaţie electronică, aceste criterii trebuie sa fie regăsite în licitaţia deschisă, în licitaţia electronică, sau în ambele faze. De asemenea, în această fază autoritatea contractantă stabileşte datele calendaristice pînă la care trebuie să se desfăşoare restul de etape.
- După publicarea procedurii de licitaţie deschisă urmează faza de înscriere a ofertanţilor la licitaţia deschisă, depunerea ofertelor iniţiale, ataşarea documentelor tehnice, economice sau de orice altă natură cerute şi răspunsul la criteriile de evaluare din această fază. Oferta de preţ trebuie introdusă criptat în această etapă.
- La finalul fazei de înscriere autoritatea contractantă trebuie sa poata efectua o evaluare tehnică a ofertanţilor înscrişi, urmată de o evaluare financiară. Sistemul trebuie sa permita ca evaluarea sa se realizeze pe baza elementelor introduse de ofertanţi în faza de înscriere.

În funcţie de necesităţi, autoritatea contractantă trebuie sa poata suspenda pe o perioadă oarecare licitaţia deschisă sau licitaţia electronică, urmînd la ca revenirea din suspendare datele calendaristice să fie decalate corespunzător. Sistemul trebuie sa permita ca în cazurile prevăzute de lege, o licitaţie deschisă sa poata sa fie anulată, cu specificarea obligatorie a motivului anulării.
Ca variantă a licitaţiei deschise trebuie sa existe posibilitatea de a defini o licitaţie restrânsă, între aceleaşi coordonate, dar avînd un pas suplimentar în care ofertanţi îşi depun întîi candidatura, sînt admişi sau respinşi de către autoritatea contractantă, după care se trece la faza de depunere a ofertelor.
În momentele importante ale desfăşurării licitaţiei, aplicaţia trebuie sa trimita automat notificări de atenţionare sau informare către entităţile implicate (autorităţi contractante, ofertanţi).

Serviciul de Licitaţie restrînsă

Procedura de licitatie restransa trebuie sa poata fi initiata prin publicarea anuntului de participare si sa fie finalizata prin publicarea anuntului de atribuire, similar ca la procedura de licitatie deschisa. Din punct de vedere al sistemului licitatia restransa trebuie implementata ca o licitatie deschisa care are in plus o etapa de preselectie. In faza de preselectie sistemul trebuie sa permita depunerea si evaluarea doar a documentelor care tin de criteriile de calificare. Evaluarea la preselectie trebuie realizata in sistem prin acordarea calificativului de admis sau respins ofertantilor inscrisi. Doar ofertantii care au fost declarati admisi in faza de preselectie trebuie sa poata depune ulterior oferta tehnica si financiara. In faza de preselectie ofertantii trebuie sa se poata inscrie, retrage si reinscrie in procedura si trebuie sa poata cere clarificari. Autoritatile contractante trebuie sa poata posta clarificari, suspenda, reveni din suspendare si anula procedura. Licitatie restransa trebuie sa poata fi organizata si pe loturi si sa poata fi prevazuta cu etapa finala de licitatie electronica. Licitatia restransa trebuie sa poata fi finaliza printr-un contract de achizitie sau prin acord cadru, insa nu printr-un sistem de achizitie dinamic.

Serviciul de Licitaţie restrînsă accelerată

Licitatia restransa accelerata trebuie implementata in sistem ca o licitatia restransa cu termene reduse. Din punct de vedere tehnic nu trebuie sa existe diferente fata de o procedura de licitatie restransa in ceea ce priveste defasurarea online a acesteia.

Serviciul Dialog competitiv

Sistemul trebuie sa ofere posibilitatea autoritatilor contractante sa desfasoare proceduri de tip dialog competitiv.
Sistemul trebuie sa ofere posibilitatea desfasurarii procedurii de dialog competitiv conform legislatiei in vigoare.

Serviciul Negociere cu sau fara publicare in prealabil a unui anunt de participare

Sistemul trebuie sa ofere posibilitatea autoritatilor contractante de a desfasura procedurile de tip negociere, cu sau fara publicarea in prealabil a unui anunt de participare.
Negocierea cu publicare in prealabil a unui anunt de participare trebuie sa fie permisa la tipurile de proceduri mentionate pentru anunturile de participare si implicit pentru fisele de date (documentatiile) aferente acestor anunturi. Pentru negocierile fara publicarea in prealabil a unui anunt de participare sistemul trebuie sa permita integrarea in cadrul anunturilor de atribuire.
In cazul negocierilor cu publicarea in prealabil a unui anunt de participare trebuie sa se poata limita numarul de agenti economici invitati sa prezinte oferte sau sa participe. Verificarea indeplinirii cerintelor de catre candidati si selectarea acestora va trebui sa se realizeze in conditii de transparenta. Limitarea numarului de candidati trebuie sa se realizeze in baza unor criterii obiective (criterii de preselectie) precizate in anuntul de participare. Limitarea candidatilor are scopul de a oferi una sau mai multe solutii apte sa raspunda necesitatilor autoritatii contractante, urmand ca pe baza solutiei/solutiilor identificate candidatii sa elaboreze oferta finala. In acest scop, dupa ce se va

finaliza selectia candidatilor, procedura trebuie sa urmeze pasii mentionati in anuntul de participare, in functie de celelalte conditii stabilite.

Serviciul Negociere accelerata

Sistemul trebuie sa ofere posibilitatea autoritatilor contractante de a desfasura procedurile de tip negociere accelerata. Negocierea accelerate trebuie sa fie permisa la tipurile de proceduri mentionate pentru anunturile de participare si implicit pentru fisele de date (documentatiile) aferente acestor anunturi.
Trebuie sa se limiteze numarului de agenti economici invitati sa prezinte oferte sau sa participe. Verificarea indeplinirii cerintelor de catre candidati si selectarea acestora trebuie sa se realizeze in conditii de transparenta. Limitarea numarului de candidati trebuie sa se realizeze in baza unor criterii obiective (criterii de preselectie) precizate in anuntul de participare.
De asemenea autoritatea contractanta trebuie sa precizeze motivul pentru care s-a ales acest tip de negociere si sa specifice daca candidatii au fost deja selectati, in situatia in care candidatii au fost deja selectati, sistemul trebuie sa permita autoritatii contractante sa-i precizeze.

Serviciul Concurs de solutii

Sistemul trebuie sa ofere posibilitatea autoritatilor contractante sa desfasoare proceduri de tip concurs de solutii. Acestea constau in achizitionarea unui plan sau a unui proiect prin selectarea acestuia pe baze concurentiale de catre un juriu, cu procedura independenta in care concurentii pot obtine premii si/sau prime de participare, sau ca parte a unei alte proceduri care conduce la atribuirea unui contract de servicii, fara acordarea de premii.
Sistemul trebuie sa permida realizarea unui concursde solutii deschis sau restrans. In cazul unei proceduri restranse trebuie sa fie limitat numarul de participanti in baza unor criterii de selectie. De asemenea trebuie sa se permita precizarea numelui participantilor selectati.
Pentru a pastra transparenta informatiilor, sistemul trebuie sa permita introducerea membrilor juriului selectati. In cazul in care exista recompense/prime, acestea trebuie introduce in sistem.
Dupa declararea proiectului/planului castigator, autoritatea contractanta trebuie sa publice un anunt cu rezultatele concursului de solutii. In acest sens, aplicatia trebuie sa permita introducerea acestui tip de anunt.

Serviciul de desfasurare a fazei finale a procedurilor de atribuire prin licitatie electronică

Acest serviciu trebuie sa ofere posibilitatea autoritatilor contractante sa reduca pretul prin utilizarea metodei de licitatie electronica in faza finala a procedurilor de atribuire.
Dacă faza anterioară de licitare a fost online, autoritatea contractantă trebuie sa poata defini această licitaţie electronică, păstrînd rezultatele evaluărilor anterioare şi definind numărul, data de începere şi durata rundelor de licitare, precum şi, dacă este cazul, criteriile care vor fi licitate în fiecare rundă.
Dacă faza anterioară de licitare a fost offline, atuci la definirea licitaţiei electronice autoritatea contractantă trebuie să poata aleage ofertanţii care vor participa, precum şi valorile de preţ şi criterii tehnico-economice asociate fiecărui ofertant participant.
De asemenea, în această de fază de definire a licitaţiei electronice trebuie sa se permita fixarea unor parametri între care se va desfăşura aceasta, ca de exemplu pasul minim de licitare, posibilitatea de a opri licitaţia în cazul neîmbunătăţirii ofertelor, sau gradul pînă la care participanţii pot vedea clasamentul intermediar al licitaţiei.
În cadrul rundelor de licitare ofertanţii trebuie sa poata licita preţul (şi oricare alt criteriu tehnico-econimic care a fost definit respectiva rundă). Trebuie sa existe posibilitatea de a prelungi licitarea dincolo de ziua şi ora fixată în cazuri speciale în care se constată un interes sporit al ofertanilor în ultima perioadă de licitare.

La încheierea licitării, autoritatea contractantă trebuie sa poata realiza o ultimă evaluare a rezultatelor, după care trebuie sa poata analiza clasamentul rezultat, desemna un cîştigător şi atribui procedura.
În funcţie de necesităţi, autoritatea contractantă trebuie sa poata suspenda pe o perioadă oarecare licitaţia deschisă sau licitaţia electronică, urmînd la ca revenirea din suspendare datele calendaristice să fie decalate corespunzător. Revenirea din suspendare trebuie sa se poata realiza şi prin întoarcere într-o etapă anterioară a procedurii, nu neapărat în cea aflată în vigoare la momentul suspendării. La nevoie, trebuie sa fie posibilă şi extinderea diverselor intervale de timp implicate, respectiv definirea unor noi date calendaristice pentru anumite etape. De asemenea, în cazurile prevăzute de lege, o licitaţie deschisă trebuie sa poata fi anulată motivarea anulării fiind obligatoriu de introdus in sistem.
În momentele importante ale desfăşurării licitaţiei electronice, aplicaţia trebuie sa trimita automat notificări de atenţionare sau informare către entităţile implicate (autorităţi contractante, ofertanţi).

Serviciul Anunturi de atribuire (Contract de achizitie publica, Acord cadru, Contract de Concesiune)

Serviciul trebuie sa ofere autoritatilor contractante posibilitatea completarii anuntului de atribuire pentruuna din metodele: Contract de achizitie publica, Acord cadru, Contract de Concesiune.
Anunţul de atribuire reprezintă faza ultimă a unei proceduri, în care autoritatea contractantă trebuie sa poata stabili cîştăgătorii procedurilor, sa poata defini contractul sau contractele asociate şi sa marcheze ofertanţii cîştigători pentru fiecare contract. Orice anunţ de atribuire trebuie sa fie creat fie pornind de la o procedură deja existentă în sistem, indiferent că este contract de achiziţie, acord-cadru,concesionare sau sistem de achizitie

dinamic, fie definindu-l ca negociere fara publicarea prealabila a unui anunt de participare/selectie/concesionare, sau ca contract pentru prestarea de servicii specifice.
De asemenea, trebuie sa existe posibilitatea de a discerne pe de o parte între anunţuri de atribuire pentru utilităţi şi non-utilităţi, iar orice anunţ de atribuire trebuie sa se poata raporta la un anumit tip de legislaţie, care priveşte sau nu achiziţiile în domeniul apărării şi securităţii.
În funcţie de valoarea procedurii sau a contractelor declarate, trebuie sa existe posibilitatea validarii ulterioare a ANRMAP.

Serviciul Erate

Serviciul de erate trebuie sa ofere autoritatilor contractante posibilitatea de a defini una sau mai multe erate la orice procedura publicata in cadrul aplicatiei. Eratele trebuie sa permita adaugarea de corectii la anuntul original sau in documentele de licitare. De asemenea trebuie sa permita adauga informatii suplimentare sau completari la o procedura incompleta.
Orice erata trebuie transmisa spre publicare, dupa ce in prealabil trebuie validata de catre autoritatile desemnate pentru a verifica veridicitatea si corectitudinea informatiilor introduse. In cazul in care erata nu este validata atunci aplicatia trebuie sa permita respingerea formularului, insa trebuie sa ofere posibilitatea de a republica continutul aceleeasi erate impreuna cu modificarile efectuate.
Din momentul in care o erata este publicata, detaliile acesteia trebuie sa poata sa fie vizualizate si de catre ceilalti operatori din cadrul aplicatiei, disponibile in cadrul procedurii initiale la care face referire. Prin toate aceste modificari si inlocuiri , fie de texte, fie de date calendaristice, fie de adrese adaugate prin mecanismul eratelor, sistemul nu trebuie sa permita modificarea anunturilor originale asociate.

Serviciul de achiziţie pe loturi

Serviciul de achizitie pe loturi trebuie sa asigure autoritatilor contractante posibilitatea de desfasurare a procedurilor de achizitie pe loturi.
În cazul procedurilor de achiziţie în care se doreşte cumpărarea separată a mai multor tipuri de produse înrudite sistemul trebuie sa permita definirea procedurilor defalcat pe loturi. Un lot trebuie sa corespunda unui anume tip de produs. Trebuie sa fie posibilă definirea oricător loturi în cadrul unei proceduri, fiecare din loturi supunîndu-se condiţiilor generale definite în cazul procedurii, cum ar fi tipul de contract (furnizare, produs, servicii), tipul procedurii (licitaţie deschisă, restrînsă etc.), moneda în care este expsimtată valoarea, existenţa sau nu a unei faze finale de licitaţie electronică şi aşa mai departe. De asemenea, suma valorilor estimate ale loturilor trebuie să egaleze valoarea estimată a întregii proceduri.
Avantajul folosirii loturilor este independenţa fluxului pentru fiecare lot în parte. Astfel, ofertanţii trebuie sa se poata înscrie şi depune oferte doar pentru lotul sau loturile dorite, iar evaluările tehnice şi financiare trebuie sa se poata face separat pentru fiecare. Definirea fazei finale de licitaţie elctronică precum şi licitarea efectivă trebuie sa se poata face independent pentru fiecare lot, iar determinarea cîştigătorilor şi atribuirea contractelor trebuie sa poata sa fie realizate separat. De asemenea, suspendarea şi anularea sa se poata face atît la nivelul întregii proceduri cît şi la nivelul fiecărui lot în parte.

Serviciul de plata online

Autoritatile contractante trebuie sa poata efectua plati online pentru taxele specificate in lege privind activitatile efectuate in sistem.
Plata trebuie sa poata fi efectuata pe baza unei facturi electronice emise de sistem.
Datele din factura electronica emisa, necesare platii, trebuie sa fie preluate automat din sistem.
Autoritatea contractanta trebuie sa aiba acces la lista platilor proprii efectuate prin sistem si la detaliile aferente acestora.

Serviciul de emitere electronic a facturilor

Serviciul de emitere electronic a facturilor trebuie sa permita emiterea de facturi electronice direct din sistem.
Pe baza facturilor emise de serviciu, autoritatile contractante trebuie sa efectueze platile catre sistem.
Emiterea facturilor electronice trebuie sa se realizeze prin preluarea informatiilor existente in sistem referitoare la datele autoritatii contractanta si tarifele aferente serviciului / ilor pentru care se emite factura.
Autoritatea contractanta trebuie sa aiba acces la lista facturilor primite si a detaliilor aferente acestora.
Facturile electronice mai vechi de un anumit interval de timp trebuie sa poata fi arhivate.
Factura electronica va reprezenta echivalentul legal, in format digital al facturii clasice, astfel incat informatiile facturii sunt procesate in format electronic, semnate si marcate temporal, in conformitate cu legislatia in vigoare.
Sistemul va asigura preluarea datelorde facturare, emiterea facturilor in format electronic, semnarea electronica si marcarea temporala. Destinatarul facturii electronice va primi un exemplar al acesteia, in format PDF. Dupa transmiterea facturii electronice astfel incat sa se garanteze receptia acesteia factura va fi arhivata, de asemenea, in format electronic.

Sistem de transmitere a facturilor electronice

In vederea asigurarii nerepudierii transmiterii si receptiei facturilor electronice se va utiliza un sistem de mesagerie electronica securizata. Principalele cerinte sunt:

a) Garantarea non-repudierii trimiterii facturii de catre expeditor, prin: generarea de dovezi de expediere a mesajelor care le contin, transferul dovezii de expediere catre partile implicate stocarea de catre sistem a dovezilor de expediere a mesajelor, obtinerea dovezilor din sistem de catre partile implicate,furnizarea de mecanisme de verificare a dovezilor. Dovezile de transmitere / primire sunt semnate electronic de catre expeditor si destinatar.

b) Garantarea **momentului trimiterii** de catre server a mesajului ce contine factura electronica prin marcarea temporala a dovezii de expediere

c) Garantarea **non-repudierii primirii mesajului** de catre destinatar, prin: generarea de dovezi de primire a mesajelor, transferul dovezii de primire catre partile implicate, stocarea de catre sistem a dovezilor de primire a mesajelor, obtinerea dovezilor de primire din sistem de catre partile implicate, furnizarea de mecanisme de verificare a dovezilor

d) Garantarea momentului primirii mesajului de catre utilizator prin marcarea temporala a dovezii de primire, conform RFC 3161.

e) Garantarea identificarii sigure a expeditorului si destinatarului mesajului pe baza de certificat digital X.509 v3

f) Garantarea autenticitatii, integritatii si confidentialitatii mesajelor schimbate intre utilizatorii sistemului prin semnarea electronica si criptarea acestora

g) Verificarea in timp real a starii certificatelor utilizate pentru semnare prin OCSP conform RFC 2560, conectarea la servicii de directoare LDAP si prin utilizarea CRL si certificate digitale stocate local.

h) Filtrarea mesajelor nedorite – anti-spam

i) Arhivarea electronica a mesajelor pentru a elimina din baza de date corpurile mesajelor a caror timp de disponibilitate on-line (setat prin profilul mesajului) a expirat.

j) Jurnalizare in vederea auditarii complete a functionarii sistemului

Securizarea traficului de mesagerie dintre serverul de e-mail si clienti se va realiza atat prin protocoale standard SMTP si POP3 cat si prin implementarea protocoalelor securizate TLS (pentru SMTP si POP3) si POP3S.
Sistemul de mesagerie trebuie sa contina module care sa asigure urmatoarele functii:

a) Managementul cheilor criptografice atat in format software cat si utilizand dispozitive hardware criptografice, certificate FIPS 140-2 Level 3

b) Generarea si trimiterea de cereri OCSP la serverul OCSP

c) Verificarea si procesarea raspunsurilor primite de la serverul OCSP

d) Generarea si trimiterea de cereri de marci temporale la serverul de TimeStamp

e) Verificarea si procesarea raspunsurilor primite de la serverul de TimeStamp

f) Generare de chei simetrice de criptare

g) Criptare / decriptare simetrica (3DES/AES)

h) Anveloparea / deanveloparea datelor (PKCS#7)

i) Semnarea digitala a datelor, inclusiv marcarea temporala (PKCS#7)

j) Verificarea starii certificatelor (perioada de valabilitate, revocare, etc)

k) Codificare / decodificare ASN.1

Sistemul trebuie sa aiba la baza o aplicatie cu interfata web la care accesul utilizatorilor se va face cu certificate digital X.509 v3 emise de o autoritate recunoscuta de sistem.
Interfata trebuie sa fie in limba romana. In acest sens se vor prezenta capturi de ecran ale aplicatiei si manuale de utilizare.
Ofertantul va prezenta un angajament de la producatorul aplicatiei ca va asigura la sediul producatorului aplicatiei servicii de instruire in regim „train the trainers" pentru utilizarea si administrarea aplicatiei.
Ofertantul va prezenta un angajament de la producatorul aplicatiei ca asigura suport tehnic on-site Beneficiarului pe toata perioada contractului, inclusiv in perioada de garantie.
Ofertantul va prezenta angajamentul de la producatorul aplicatiei prin care acesta garanteaza ca asigura functionalitatile cerute prin caietul de sarcini.

Facilitate de publicare a comunicarii rezultatului procedurii

Serviciul trebuie sa permita publicarea documentului constatator in sistem si pastrarea istoricului acestuia.
Publicarea in sistem trebuie sa se faca prin completarea unui formular ce trebuie sa contina campurile specificate in legislatia in vigoare.
Sistemul trebuie sa ofere posibilitatea realizarii de statistici pe baza informatiilor din documentele constatatoare.

Serviciul avansat de cautare si raportare a informatiilor publice

Serviciul avansat de cautare si raportare a informatiilor publice trebuie sa permita autoritatilor contractante posibilitatea de primire a unor rapoarte complexe.
Autoritatea contractanta trebuie sa poata defini filtrele pe baza carora se genereaza rapoartele in baza unor reguli avansate deja definite.
Accesul la rapoarte trebuie sa fie realizat din cadrul zonei de portal accesebila autoritatilor contractante.
Rapoartele trebuie sa ofere doar informatiile la care autoritatea contractanta are acces.
Pe baza regulilor deja definite, autoritatea contractanta trebuie sa poata genera rapoarte pentru subseturi de date si diferite intervale de timp.

Serviciul avansat de notificări automate

Sistemul trebuie sa dispuna de un serviciu avansat de generare si transmitere automata de notificari care sa permita informarea autoritatilor contractante cu privire la actiunile / activitatile relevante care urmeaza sa se intample sau care s-au intamplat deja, aflate in stransa legatura cu activitatea desfasurata de aceste entitati in sistem. Aceste notificari trebuie sa fie generate in mod automat de catre aplicatie si sa se transmita pe adresa de e-mail a autoritatii contractante setata in profilul acesteia. Ca alternativa de backup, notificarea trebuie sa poata fi accesata si din sistem, pentru a acoperi cazul in care din diverse motive e-mailul nu ajuns la destinatar. Aplicatia trebuie sa genereze urmatoarele tipuri de notificari: notificari de confirmare a actiunilor (de ex: la publicarea anuturilor, la anularea sau atribuirea procedurilor, la finalizarea evaluarii sau deliberarii etc.), notificari de avertizare (de ex: la expirarea certificatului digital), notificari de la administratorul sistemului (notificari de instiintare pe care le transmite Operatorul AADR sau alt tip de entitate cu acest rol). Notificarile de confirmare ale actiunilor trebuie sa contina intotdeauna in mesajul lor datele de identificare ale operatiunii (de ex: numarul anuntului, data publicarii, denumirea contractului, denumirea castigatorului etc).

Serviciul contracte

Serviciul contracte trebuie sa permita autoritatilor contractante completarea informatiile referitoare la contractele semnate in urma finalizarii procedurilor de achizitie.
Trebuie sa permita gestionarea tuturor tipurilor de contracte (contract de achizitie, acord cadru etc) incheiate in urma procedurilor de achizitie publica derulate prin sistem.
Autoritatea contractanta trebuie sa aiba posibilitatea gestionarii actelor aditionale aferente contractelor semnate.
Prin intermediul serviciului, autoritatea contractanta trebuie sa poata vizualiza in orice moment, in cadrul zonei de portal accesibila autoritatilor contractante, un contract impreuna cu toate documentele aferente.
O autoritate contractanta trebuie sa aiba acces doar la contractele incheiate de aceasta in urma derularii procedurilor de achizitie publica derulate prin sistem.
Contractele gestionate trebuie sa contina informatii preluate din sistem (datele autoritatii contractante si datele ofertantului), din procedura de achizitie publica derulata de autoritatea contractanta si sa permita adaugarea informatiilor specifice contractului.
Serviciul de contracte trebuie sa se interconecteze cu Serviciul Dosarul achizitiei din cadrul SEAP.

In cadrul unui contract trebuie sa poate fi gestionate informatii referitoare la etape, termene etc.
Pentru fiecare etapa din contract, sistemul trebuie sa permita adaugarea de documente care sa ateste incheierea acesteia (PV receptie etapa, PV receptie finala etc).
Pe baza informatiilor din contract, sistemul trebuie sa transmita automat notificari partilor contractante (autoritate contractanta si ofertant).
Autoritatea contractanta trebuie sa poata vizualiza in orice moment starea unui contract (in derulare, suspendat, rezilizat, in garantie, in mentenanta etc).
Autoritatea contractanta trebuie sa poata vizualiza lista contractelor incheiate.

Serviciu extins de raportare si statistici

Serviciul extins de raportare si statistici trebuie sa permita autoritatilor contractante sa obtina rapoarte si statistici predefinite prin utilizarea informatiilor nou introduce in sistem.
O autoritate contractanta trebuie sa aiba acces doar la informatiile proprii sau la cele publice.
Rapoartele trebuie sa fie disponibile in zona de portal accesibila autoritatilor contractante.

Servicii web extinse pentru interoperabilitate

Serviciile web trebuie sa asigure interoperabilitatea intre sistem si sistemele informatice ale autoritatilor contractante.
Sistemul trebuie sa permita prin intermediul unui seviciu web preluarea unui contract (informatiilor) din sistemul informatic al autoritatii contractante.
Sistemul trebuie sa permita prin intermediul unui serviciu web exportul unui contract (informatiilor) din sistem.
Sistemul trebuie sa permita prin intermediul unui serviciu web exportul facturii electronice generate de sistem si a atributelor aferente acesteia.

Integrare cu serviciul pentru gestiunea fiselor de date

Sistemul trebuie sa permita managementul fiselor de date pentru procedurile de achizitie desfasurate in sistem prin intermediul serviciului pentru gestiunea fiselor de date.
O fisa de date initiata de autoritatea contractanta in sistem trebuie sa fie transmisa automat catre Serviciul pentru gestionarea fiselor de date.
Dupa rezolutionarea fisei de date in serviciul pentru gestionarea fiselor de date, sistemul trebuie sa primeasca automat informatii privind rezolutia acordata si toate informatiile associate in baza carora autoritatea fie va trebui sa modifice informatiile din fisa de date, fie va putea trece la urmatorul pas din flux.
Autoritatea contractanta trebuie sa aiba posibilitatea sa completeze / corecteze informatiile in sectiunile solicitate si sa asocieze documente la solicitarea institutiei cu rol in reglementare si control al procedurilor de achizitii publice.
Autoritatea contractanta trebuie sa aiba posibilitatea sa retransmita spre aprobare fisa de date modificata catre serviciul pentru gestionarea fiselor de date si sa primeasca informatii actualizate pana la aprobarea fisei de date de catre ANRMAP.
Transmiterea fiselor de date in Serviciul pentru gestiunea fiselor de date trebuei sa tina cont de mecanismul de repartizare automata multicriteriala.
Intergrarea trebuie sa faciliteze utilizatorilor ANRMAP accesul la actualizarile realizate de autoritatea contractanta la nivelul fisei de date si sa evidentieze trasabilitatea fisei de date.
Integrarea trebuie sa asigure cu transmiterea cu prioritate a fiselor de date refacute de autoritatea contractanta.

Actualizare procedura de achizitie in domeniul apararii si securitatii (Directiva 2009/81/CE)

Sistemul trebuie sa permita definirea procedurilor de achizitie in domeniul apararii si securitatii astfel incat sa respecte prevederile mentionate in directiva 2009/81/CE. La implementare trebuie sa se foloseasca formularele si fluxurile specificate prin legislatia in vigoare si sa se adapteze in functie de particularitatile din domeniul apararii si securitatii pentru fiecare tip de anunt. De exemplu, in cazul contractelor de prestari de servicii care intra sub incidenta directivei si in scopuri de monitorizare, serviciile trebuie clasificate in categorii care corespund diferitelor rubrici ale nomenclaturii CPV si regrupate in doua anexe. Anunturile pentru care trebuie permisa definirea acestor tipuri de proceduri sunt urmatoarele: anunturile de intentie, anunturile de participare, anunturile de atribuire, cererile de oferta. Pentru concesionari si concursuri de solutii in sistem nu trebuie sa existe optiunea pentru domeniul apararii.
Anunturile de acest tip trebuie validate de catre ANRMAP, insa nu trebuie validate fisele de date asociate.
Deoarece aceasta categorie de achizitii are un caracter deosebit de sensibil si necesita un nivel foarte ridicat de confidentialitate, sistemul trebuie sa permita restrictionarea accesului operatorilor, de exemplu la nivel de vizualizare a informatiilor introduse.

3.2.2 Servicii pentru ofertanti

Serviciul profil ofertant

Serviciul profil ofertant trebuie sa permita utilizatorilor accesul la urmatoarele categorii de informatii:

- elementele de identificare ale entităţii: nume, cod de identificare fiscală, număr de înrergistrare la registrul comerţului, reprezerntantul legal, banca şi contul bancar
- adresele folosite de entitate trebuie sa contina informatiile uzuale pentru o adresa (stradă, număr, persoană de contact etc.); trebuie sa existe minim o adresa de contact;
- lista codurilor CAEN - tipurile de activităţi în care este încadrată entitatea
- un set de documente de referinţă
- lista utilizatorilor unei entitati si rolurile asociate acestora
- o serie de informaţii referitoare la participarile preplătite ale ofertantului, defalcate în participări la proceduri si pozitii de catalog în cadrul cumpărărilor directe

Serviciul de participare la procedurile de achizitie initiate de Autoritatea Contractanta

Acest serviciu trebuie sa permita participarea ofertantilor la toate tipurile de proceduri initiate de autoritatile contractante in sistem si realizarea actiunilor specifice fiecarei proceduri.
Orice ofertant trebuie sa se poata înscrie în cadrul unei proceduri online, indiferent că este vorba de anunţ de participare sau invitaţie de participare. Înscrierea presupune plata unei taxe, realizată prin consumarea unei participări preplătite a respectivului ofertant. Orice ofertant trebuie sa se poata retrage şi să se poata reînscrie într-o procedură, atîta vreme cît nu depăşeşte data limită a fazei de înscriere. Înscrierea la o procedură defalcată pe loturi trebuie sa necesite în mod suplimentar înscrierea explicită pe lotul sau loturile dorite, fără ca aceasta să impună plata unei taxe suplimentare. Similar, în cazul licitaţiilor restrînse trebuie sa fie considerată înscriere (şi trebuie sa se taxeaza ca atare) depunerea candidaturii la procedură.
Înscrierea sau depunerea candidaturii în cadrul procedurii trebuie sa fie un pas necesar dar nu şi suficent pentru participarea efectivă la procedură, ofertanţii trebuind să depună oferte de preţ, să răspundă la criteriile de evaluare şi la întebările autorităţii contractante, şi să încarce documentele de calificare necesare. Neîndeplinirea acestor condiţii trebuie sa poata duce la eliminarea automată din procedură a ofertantului. Orice participant la procedură care nu a fost eliminat automat trebuie sa fie ulterior evaluat din punct de vedere tehnic şi financiar. Sistem trebuie sa permita ca ofertantul sa fiedeclarat fie admis fie respins.

În funcţie de tipul procedurii, trebuie sa existe un număr minim de participanţi care trebuie să fie declaraţi admişi pentru ca procedura să poată continua şi să nu fie anulată administrativ.

Serviciul avansat de cautare si raportare a informatiilor publice

Serviciul avansat de cautare si raportare a informatiilor publice trebuie sa permita ofertantilor posibilitatea de primire a unor rapoarte complexe.
Ofertantii trebuie sa poata defini filtrele pe baza carora se genereaza rapoartele in baza unor reguli avansate deja definite.
Accesul la rapoarte trebuie sa fie realizat din cadrul zonei de portal accesebila ofertantilor.
Rapoartele trebuie sa ofere doar informatiile la care ofertantul are acces.

Serviciul de plata online

Ofertantii trebuie sa poata efectua plati online pentru taxele specificate in lege privind activitatile efectuate in sistem.
Plata trebuie sa poata fi efectuata pe baza unei facturi electronice emise de sistem.
Datele din factura electronica emisa, necesare platii, trebuie sa fie preluate automat din sistem.
Ofertantii trebuie sa aiba acces la lista platilor proprii efectuate prin sistem si la detaliile aferente acestora.

Serviciul de emitere electronica a facturilor

Serviciul de emitere electronic a facturilor trebuie sa permita emiterea de facturi electronice direct din sistem.
Pe baza facturilor emise de serviciu, ofertantii trebuie sa efectueze platile catre sistem.
Emiterea facturilor electronice trebuie sa se realizeze prin preluarea informatiilor existente in sistem referitoare la datele ofertantilor si tarifele aferente serviciului / ilor pentru care se emite factura.
Ofertantii trebuie sa aiba acces la lista facturilor primite si a detaliilor aferente acestora.
Facturile electronice mai vechi de un anumit interval de timp trebuie sa poata fi arhivate.

Serviciul Alocare automata a participarilor preplatite pentru plati electronice

Sistemul trebuie sa asigure alocarea automata in sistem, fara interventia manuala a unui operator, a participarilor preplatite de catre ofertantii care au efectuat plata online. Serviciul trebuie sa se integreze cu sistemul de plati on-line sa permita identificarea platilor pentru tipurile de participari preplatite si sa permita plata proportionala cu pretul unei participari.

Serviciul avansat de notificari automate

Sistemul trebuie sa dispuna de un serviciu avansat de generare si transmitere de notificari care sa permita informarea ofertantilor cu privire la actiunile / activitatile relevante care urmeaza sa se intample sau care s-au intamplat deja, aflate in stransa legatura cu activitatea desfasurata de aceste entitati in sistem. Aceste notificari trebuie sa fie generate in mod automat de catre aplicatie si trebuie sa se transmita pe adresa de e-mail a ofertantilor setata in profilul acesteia. Ca alternativa de backup, notificarea trebuie sa poata sa fie accesata si din sistem, pentru a acoperi cazul in care din diverse motive e-mailul nu ajuns la destinatar. Notificarile de confirmare ale actiunilor trebuie sa contina intotdeauna in mesajul lor datele de identificare ale operatiunii (de ex: numarul anuntului, data publicarii, denumirea contractului, denumirea castigatorului etc).

Serviciul de informare privind anunturile pe criterii avansate de interes

Ofertantii trebuie sa aiba posibilitatea configurarii de alerte prin care sa fie informati cu privire la noutatile din sistem. In sistem trebuie existe doua tipuri de notificari: prin raportari periodice si contextuale. Raportarile periodice trebuie sa permita configurarea de alerte pe baza unor sabloane predefinite de raportari si a criteriilor de interes selectate. Un exemplu de alerta ar fi anunturi de participare publicate pentru anumite codui CPV in ultima saptamana. Pentru fiecare raportare trebuie sa se permita alege periodicitatii generarii: zilnic, saptamanal. Sabloanele de rapoartari trebuie sa cuprinda: anunturi de intentie, participare, atribuire etc. Criteriile de interes pot fi de exemplu: codurile CPV, autoritatea contractanta initiatoare, tipul de contract sau de procedura. Alerta trebuie sa se poata primi prin e-mail si sa contina un raport cu informatiile solicitate conform criteriilor de interes setate, si sa reprezinte noutatile de la ultima generare a alertei. Notificarile contextule trebuie sa sermita abonarea la un anumit anunt pentru a primi alerte la fiecare modificare importanta care vizeaza respectivul anunt. Abonarea trebuie sa se poata face din detaliul anuntului respectiv. Alertele trebuie sa se primeasca prin e-mail. Printre evenimentele generatoare de alerte se numara: suspendarea, anulara sau atribuirea procedurii, postarea de clarificari sau erate etc. Un ofertant trebuie sa poata oricand sa se dezaboneze de la primirea acestor alerte.

Serviciul contracte

Serviciul contracte trebuie sa permita ofertantilor validarea informatiile referitoare la contractele semnate in urma finalizarii procedurilor de achizitie.
Ofertantii trebuie sa aiba posibilitatea validarii actelor aditionale aferente contractelor semnate.
Un ofertant trebuie sa aiba acces doar la contractele incheiate de aceasta in urma derularii procedurilor de achizitie publica derulate prin sistem.
Trebuie sa permita validareaa tuturor tipurilor de contracte (contract de achizitie, acord cadru etc) incheiate in urma procedurilor de achizitie publica derulate prin sistem.
Contractele la care ofertantul are acces trebuie sa contina informatii preluate din sistem (datele autoritatii contractante si datele ofertantului), datele din procedura de achizitie publica derulata prin sistem si informatiilor specifice contractului adaugate de autoritatea contractanta cu care a incheiat contractul si validate de catre ofertant.
Ofertantul trebuie sa poata valida si vizualiza informatii referitoare la etape, termene etc si documente aferente contractului (PV receptie etapa, PV receptie finala etc), incheiate intre acesta si autoritatea contractanta pe toata perioada de derulare a acestuia.
Pe baza informatiilor din contract, sistemul trebuie sa transmita automat notificari partilor contractante (autoritate contractanta si ofertant).
Ofertantul trebuie sa poata vizualiza in orice moment starea unui contract (in derulare, suspendat, rezilizat, in garantie, in mentenanta etc).
Ofertantul trebuie sa poata vizualiza lista contractelor incheiate.

Serviciu extins de raportare si statistici

Serviciul extins de raportare si statistici trebuie sa permita ofertantilor sa obtina rapoarte si statistici predefinite prin utilizarea informatiilor nou introduce in sistem.
Un ofertant trebuie sa aiba acces doar la informatiile proprii sau la cele publice.
Rapoartele trebuie sa fie disponibile in zona de portal accesibila ofertantilor.

Servicii web extinse pentru interoperabilitate

Serviciile web trebuie sa asigure interoperabilitatea intre sistem si sistemele informatice ale ofertantilor.
Sistemul trebuie sa permita prin intermediul unui serviciu web exportul unui contract (informatiilor) din sistem.
Sistemul trebuie sa permita prin intermediul unui serviciu web exportul facturii electronice generate de sistem si a atributelor aferente acesteia.

Serviciul de informare pentru dispozitive mobile

Serviciul de informare pentru dispositive mobile trebuie sa ofere ofertantilor posibilitatea de acces de pe dispositive mobile la principalele functionalitati ale sistemului.
Ofertant trebuie sa poata accesa informatiile disponibile prin accesarea de pe dispozitivul mobil a informatiilor proprii.

Serviciul trebuie sa permita definirea de notificari / instiintari pe baza unor criterii care trebuie sa fie accesibile de pe dispozitivul mobil.
Serviciul trebuie sa permita ofertantilor participarea in cadrul procedurilor de achizitie prin intermediul dispozitivelor mobile.

3.2.3 Servicii pentru institutii cu rol in reglementare si control al procedurilor de achizitii publice

Serviciul Profil Institutie

Serviciul profil institutie trebuie sa permita utilizatorilor accesul la urmatoarele categorii de informatii:

- elementele de identificare ale entităţii: nume, cod de identificare fiscală, număr de înrergistrare la registrul comerţului, reprezerntantul legal, banca şi contul bancar
- adresele folosite de entitate trebuie sa contina informatiile uzuale pentru o adresa (stradă, număr, persoană de contact etc.); trebuie sa existe minim o adresa de contact;

Serviciul avansat de cautare si raportare a informatiilor publice

Serviciul avansat de cautare si raportare a informatiilor publice trebuie sa permita institutiilor cu rol in reglementarea si controlul procedurilor de achizitii publice posibilitatea de primire a unor rapoarte complexe.
Institutiile cu rol in reglementarea si controlul procedurilor de achizitii publice trebuie sa poata defini filtrele pe baza carora se genereaza rapoartele in baza unor reguli avansate deja definite.
Accesul la rapoarte trebuie sa fie realizat din cadrul zonei de portal accesebila institutiilor cu rol in reglementarea si controlul procedurilor de achizitii publice.
Rapoartele trebuie sa ofere doar informatiile la care institutiile cu rol in reglementarea si controlul procedurilor de achizitii publice are acces.

Serviciul avansat de notificari automate

Sistemul trebuie sa includa un serviciu avansat de generare si transmitere de notificari care sa permita informarea institutiilor cu rol in reglementarea si controlul procedurilor de achizitii publice cu privire la actiunile / activitatile relevante care urmeaza sa se intample sau care s-au intamplat deja, aflate in stransa legatura cu activitatea desfasurata de aceste entitati in sistem. Aceste notificari trebuie sa fie generate in mod automat de catre aplicatie si sa se transmita pe adresa de e-mail a entitatii setata in profilul acesteia. Ca alternativa de backup, notificarea trebuie sa poata fi accesata si din sistem, pentru a acoperi cazul in care din diverse motive e-mailul nu ajuns la destinatar.

Servicii pentru Departamentul pentru proiecte de infrastructura si investitii straine

Serviciul trebuie sa permita utilizatorilor Departamentului pentru proiecte de infrastructura si investitii straine sa realizeze in sistem actiunile stabilite prin legislatiea in vigoare pe parcursul desfasurarii procedurilor de achizitie.
Serviciul trebuie sa ofere posibilitatea verificarii si monitorizarii conform pragurilor si procedurilor prevazute in legislatia in vigoare privind tipurilor de proceduri care intra sub incidenta Departamentului pentru proiecte de infrastructura si investitii straine.

Integrare cu serviciul UCVAP pentru urmarirea achizitilor

Integrarea cu serviciul UCVAP trebuie realizata in vederea desfasurarii activitatilor de avizare si control in cadrul procedurilor de achizitie desfasurate prin sistem.
Prin serviciul UCVAP trebuie sa se realizeaze preluarea automata din sistem a informatiilor necesare in vederea realizarii analizei de risc pentru procedurile de achizitii care fac obiectul verificarii UCVAP, conform pragurilor valorice stabilite prin lege si transmiterea acestor date la UCVAP, impreuna cu gradul de risc calculat pentru fiecare procedura, prin aplicarea algoritmului analizei de risc.

Servicii web extinse pentru interoperabilitate

Serviciile web trebuie sa asigure interoperabilitatea intre sistem si sistemele informatice ale institutiilor cu rol in reglementare si control al procedurilor de achizitii publice.

Integrare cu serviciul pentru gestiunea fiselor de date

Sistemul trebuie sa permita avizarea fiselor de date pentru procedurile de achizitie noi desfasurate in sistem prin intermediul serviciului pentru gestiunea fiselor de date.
Institutiile cu rol in reglementare si control al procedurilor de achizitii publice trebuie sa avizeze fisele de date prin serviciul pentru gestionarea fiselor de date, in functie de aria de competenta.
O fisa de date respinsa de institutia cu rol in reglementare si control al procedurilor de achizitii publice va fi reevaluata de aceasta in serviciul pentru gestiunea fiselor de date.
Sistemul trebuie sa permita transmitere catre fiecare institutie cu rol in reglementarea si controlul al procedurilor de achizitii publice doar a fiselor de date pe care acestea au responsabilitatea sa le evalueze.
De asemenea, sistemul trebuie sa permita preluarea distincta a informatiilor privind evaluarea fiselor de date din serviciul pentru gestiunea fiselor de date pentru fiecare tip de utilizator (institutie) in parte.
Mecanismul de repartizare automata implementat in sistem va trebui sa distribuie diferentiat fisele de date catre institutiile cu rol in in reglementarea si controlul al procedurilor de achizitii publice in functie de competentele acestora.

Solutie de raportate extinsa pentru institutiile cu rol in reglementarea si controlul procedurilor de achizitii publice

Serviciul extins de raportare si statistici trebuie sa permita institutiilor cu rol in reglementare si control al procedurilor de achizitii publice sa obtina rapoarte si statistici predefinite prin utilizarea informatiilor nou introduse in sistem.

O institutie cu rol in reglementare si control al procedurilor de achizitii publice trebuie sa aiba acces doar la informatiile necesare desfasurarii activitatiilor prevazute de lege .

Rapoartele trebuie sa fie disponibile in zona de portal accesibila institutiilor cu rol in reglementare si control al procedurilor de achizitii publice.

3.2.4 Servicii pentru operatorii AADR

Serviciul Profil Operator AADR

Serviciul profil Operator AADR trebuie sa permita utilizatorilor accesul la urmatoarele categorii de informatii:

- elementele de identificare ale entităţii: nume, cod de identificare fiscală, număr de înregistrare la registrul comerţului, reprezerntantul legal, banca şi contul bancar
- adresele folosite de entitate trebuie sa contina informatiile uzuale pentru o adresa (stradă, număr, persoană de contact etc.); trebuie sa existe minim o adresa de contact.

Serviciu extins de raportare si statistici

Serviciul extins de raportare si statistici trebuie sa operatorilor AADR sa obtina rapoarte si statistici predefinite prin utilizarea informatiilor nou introduse in sistem.

Operatorul AADR trebuie sa aiba acces doar la informatiile din sistem, avand rol de administrator al acestuia.

Rapoartele trebuie sa fie disponibile in zona de portal accesibila operatorilor AADR.

Serviciul de Arhivare documente electronice

Serviciul de arhivare documente electronice trebuie sa permita arhivarea tuturor documentelor vechi, care nu mai sunt accesate frecvent.

Termenele de arhivare stabilite trebuie sa fie corelate cu termenele stabilite prin lege.

Sistemul trebuie sa ofere posibilitatea de acces la acestea pe baza de cerere.

Operatorul AADR trebuie sa poata readuce din arhiva un document pe baza de cerere primita de la o autoritate contractanta, ofertant sau reprezentant al unei institutii cu drept de reglementare si control a procedurilor de achizitii publice.

Serviciul de transmitere automata la OJEU a informatiilor din sistem

Sistemul trebuie sa permita transmiterea automata a anunturilor la ojeu, precum si instiintarea utilizatorilor cu privire la statusul transmiterii acestora prin intermediul serviciului de transmitere automata la OJEU a informatiilor din sistem. Anunturile cu valori peste pragurile prevazute in legislatia achizitiilor publice trebuie sa fie automat selectate de sistem pentru transmiterea la OJEU. Sistemul trebuie sa ofere posibilitatea transmiterii la ojeu si a anuturilor care nu depasesc pragurile legale, daca autoritatea contractanta opteaza in mod explicit pentru publicarea lor in jurnal oficial al uniunii europene. In vederea transmiterii anunturilor la OJEU, fiecare anunt trebuie sa fie convertit intr-un fisier XML, care va trebui sa respecte o anumita forma impusa de OJEU. Maparea informatilor din anunturi, precum si gestiunea transmiterii acestora la OJEU trebuie sa se faca prin prin acest serviciu, care va fi responsabil cu impachetarea informatiilor din anunturi, crearea arhivelor si transmiterea acestora la OJEU prin posta electronica. Maparea trebuie sa permita punerea in corespondenta a informatilor din anuntul definit in sistem cu elemntele schemei de validare furnizate de OJEU. Publicarea in sistem a anunturilor cu transmitere la OJEU tebuie sa se faca doar dupa transmitetea acestora la OJEU. Fiecare anunt trebuie sa aiba propriul formular. In sistem trebuie sa fie prevazute formulare pentru anunturi de intentie, participare, atribuire defalcat pe utilitati, non utilitati si aparare, concesionari, concurs de soltii sau anunt simplificat la sistemul dinamic de achizitii. Autoritatea contractanta care a transmis spre publicare anuntul trebuie sa poata avea acces oricand din sistem la informatia cu privire la statusul anuntului: daca este in asteptare trimitere la OJEU, daca a fost transmis sau s-a publicat in sistem.

Serviciu de auditare actiuni in sistem

Serviciul de auditare actiuni in sistem trebuie sa permita operatorilor AADR cu drept special sa filtreze si sa vizualizeze operatiile efectuate in sistem in functie de criteriile selectate.

Sistemul trebuie sa auditeze toate actiunile principale efectuate in sistem de catre toti utilizatorii inregistrati.

Auditarea actiunilor in sistem trebuie sa se realizeze pe tipuri de actiuni, pe procedura si pe tip de actor inregistrat in sistem.

Sistemul trebuie sa permita arhivarea informatiilor referitoare la auditarea actiunilor in sistem dupa o anumita perioada e timp.

In sistem trebuie sa existe un set de criterii pe baza carora operatorul AADR vizualizeaza operatiile efectuate in sistem.

Informatiile referitoare la operatiile efectuate in sistem trebuie sa fie disponibile in zona de portal accesibila operatorilor AADR si numai operatorii AADR cu drept special trebuie sa aiba acces la aceasta categorie de informatii.
Sistemul trebuie sa permita aducerea din arhiva a unui set de informatii referitoare la auditarea actiunilor in sistem, pe baza cererii efectuate de Operatorul AADR.

Serviciu pentru cercetarea opiniilor utilizatorilor

Serviciul pentru cercetarea opiniilor utilizatorilor trebuie sa ofere operatorilor AADR un mecanism prin care se pot defini si solicita opinii din parte utilizatorilor sistemului.
Serviciul trebuie sa permita definirea unui set de intrebari si raspunsuri predefinite.
Sistemul trebuie sa permita selectarea categoriei de utilizatori careia se adreseaza intrebarile.
Sistemul trebuie sa permita operatorului AADR sa realizaze statistici pe baza raspunsurilor primite de la utilizatori.

3.2.5 Servicii publice cetateni

Informatii publice in domeniul achizitiilor publice

Serviciul Informatii publice in domeniul achizitiilor publice trebuie sa ofere prin cadrul portalului public acces la informatiile publice pentru orice persoana fizica care nu este inregistrata in sistem.
Portalui trebuie sa permita accesul oricarei persoane fizice care nu este inregistrata in sistem la informatiile publice din sistem, conform legislatiei in vigoare.

3.2.6 Alte servicii

Serviciu de tip colaborativ si de instruire on-line a utilizatorilor

Acest serviciu trebuie sa asigure o platforma colaborativa pentru instruirea on-line a utilizatorilor pentru asigurarea folosirii optime a tuturor serviciilor noi si actualizalor ce se vor realiza in urma modificarilor legislative sau organizationale. Cerinte detaliate privind acest serviciu sunt detaliate in capitolul software de baza.

Serviciu autoritate de certificare

Acest serviciu va asigura gestiunea completa a certificatelor digitale necesare asigurarii securitatii sistemului informatic SICAP. Serviciul va fi implementat prin intermediul unei autoritati de certificare care va gestiona certificatelor digitale de semnatura electronica criptare si autentificare – se vor oferi licente pentru un numar nelimitat de utilizatori – cu urmatoarele componente:
Modul de gestiune a certificatelor digitale;

Modul de validare online a starii certificatului;

Modul de marcare temporala;

Modul de recuperare a cheilor private de criptare;

Modul de administrare a dispozitivelor criptografice ale utilizatorilor.

Se va realiza migrarea de la infrastructura PKI existenta pentu a se asigura continuitatea serviciilor asociate certificatelor digitale emise

Serviciu securizat de management al cererilor si solicitarilor din partea utilizatorilor

Acest serviciu joaca rol de suport pentru alte servicii/module din cadrul SICAP si trebuie sa fie un instrument de management al documentelor si workflow securizat, ce asigura circulatia documentelor conform fluxurilor definite. Cerinte detaliate privind acest serviciu sunt detaliate in capitolul software de baza.

Serviciu de securitate sistem

Infrastructura de securitate informatica implementata va asigura mecanismele necesare schimbului protejat de informatii. In acest sens se va asigura implementarea urmatoarelor componente:

- Infrastructura de chei publice (PKI – Public Key Infrastructure), asa cum a fost descrisa anterior
- Accesul la sistem utilizand autentificare de pe terminale mobile
- Software pentru validarea documentelor semnate electronic și a mărcii temporale
- Software pentru semnarea automatizată a documentelor electronice

- Dispozitive criptografice

Serviciul de securitate va permite protejarea tranzactiilor realizate si va asigura accesul controlat la resurse.

Integrare cu serviciile dezvoltate prin proiectul „Servicii de extindere S.E.A.P. prin trecerea la un sistem dinamic si oferirea facilitatii de interoperabilitate pentru utilizatorii sistemului"

Sistemul trebuie sa asigure integrarea cu Serviciul de management al planurilor/programelor anuale de achiziţii publice prin asocierea procedurilor derulate prin acesta.
Initierea tuturor procedurilor din sistem trebuie sa se realizeze corelat cu informatiile gestionate de Serviciul de management al planurilor/programelor anuale de achiziţii publice.
Sistemul trebuie sa asigure integrarea cu Sistemul de achizitie dinamic.
Sistemul trebuie sa asigure integrarea cu Serviciul dosarul companiei prin gestionarea in cadrul Dosarului companiei a documentelor proprii ofertantilor, documente gestionate prin intermediul acestuia.
Pe parcursul derularii procedurilor de achizitie, sistemul trebuie sa ofere Ofertantilor posibilitatea utilizarii documentelor gestionate prin intermediul Dosarului companiei, in toate etapele de desfasurare ale acestora.
Sistemul trebuie sa asigure integrarea cu Dosarul electronic al achizitiei prin preluarea in dosarul electronic al achizitiei a documentelor procedurilor de achizitie derulate prin acesta.
Sistemul trebuie sa asigure integrarea cu Serviciul de marcare temporala pentru documente prin marcarea temporala a documentelor gestionate de acesta.
Sistemul trebuie sa asigure integrarea cu Serviciul de management documente si workflow securizat.
Sistemul trebuie sa permita transmiterea colectiilor de documente istorice catre Serviciul de management documente si workflow securizat in vederea arhivarii.
Ofertantul trebuie sa descrie in detaliu modul de integrare cu serviciile dezvoltate prin proiectul „Servicii de extindere S.E.A.P. prin trecerea la un sistem dinamic si oferirea facilitatii de interoperabilitate pentru utilizatorii sistemului".

Servicii de acces la sistem utilizand autentificarea de pe terminale mobile

Accesul la sistem se va realiza centralizat folosind certificate digitale atat emise de infrastructura PKI a sistemului cat si certificate calificate emise de furnizori publici de servicii de certificare acreditati in conditiile legii nr 455/2001. Sistemul trebuie sa asigure ergonomie sporita pentru utilizatori iar accesul se va realiza atat de pe calculator cat si de pe dispozitivele mobile de tip telefoane inteligente sau tablete.
Certificatul digital folosit pentru autentificare trebuie sa poata fi stocat:
Pentru utilizarea de pe calculator, permitand ambele posibilitati:

Pe un dispozitiv sigur de pastrare a certificatului, de tip smart card, conectat la calculator

In memoria calculatorului, in format PKCS#12

Pentru utilizarea de pe echipamentul mobil, permitand ambele posibilitati:

Pe un dispozitiv sigur de pastrare a certificatului, de tip smart card, conectat la echipamentul mobil

In memoria echipamentului mobil, in format PKCS#12

Procesul de autentificare trebuie sa permita implementarea tuturor scenariilor prezentate mai jos, utilizand conexiune SSL:
Acces de pe calculator si autentificare cu certificat digital aflat pe un dispozitiv criptografic conectat la calculator sau un certificat stocat pe calculator in format PKCS#12

Acces de pe calculator si autentificare cu certificat digital aflat pe un dispozitiv criptografic conectat la echipamentul mobil sau un certificat stocat pe echipamentul mobil in format PKCS#12

Acces de pe echipamentul mobil si autentificare cu certificat digital aflat pe un dispozitiv criptografic, conectat la echipamentul mobil sau un certificat stocat pe echipamentul mobil in format PKCS#12

Pentru a oferi un context unitar de autentificare la aplicatiile web este necesara integrarea componentei de autentificare utilizand certificate dispozitive mobile cu aplicatia existenta care realizeaza operatiunile de autentificare si autorizare. Aplicatia existenta ofera urmatoarele functionalitati:
Autentificarea utilizatorilor pe baza certificatului digital X.509 v3 detinut. Certificatul digital trebuie sa fie emis de o autoritate de certificare de incredere

Autorizarea utilizatorilor pe baza listelor de acces detinute de acest serviciu.

Autorizarea utilizatorilor pe baza extensiilor din certficat digital, inclusiv ale celor private definite intern de beneficiar

Criptarea canalului de comunicatie intre clientul web (browser) si serviciul de autentificare utilizand SSL (HTTPS)

Single Sign On la aplicatii. Odata autentificat cu certificatul digital si credentiale, utilizatorului nu trebuie sa i se mai ceara alte credentiale, pentru oricare dintre aplicatiile ce urmeaza a fi accesate.

Aplicatia asigura urmatoarele optiuni:
Validarea certificatelor digitale pe baza CRL-urilor publicate pe LDAP

Validarea certificatelor digitale pe baza protocolului OCSP conform RFC 2560

Contexte de securitate diferite in functie de zona aplicatiei accesata. Astfel in cadrul aplicatiei web pot fi prezentate informatii publice pentru care nu este necesara autentificarea. Solutia trebuie sa permita conexiuni http si https in functie de aceste contexte.

Configurarea autoritatilor de certificare considerate de incredere

Configurarea credentialelor utilizatorilor pentru aplicatiile accesate(utilizator si parola, emitent si numar serial certificat digital).

Configurarea metodelor de autentificare utilizate de aplicatiile accesate (Basic Authentication, Form authentication, LDAP)

Functionalitatile si optiunile existente trebuie sa fie oferite si in momentul autentificarii folosind dispozitivele mobile.
Pentru accesul la aplicatiile web, folosind un dispozitiv mobil de tip smartphone sau tableta, un utilizator trebuie sa parcurga urmatorul flux:
Introduce adresa aplicatiei web pe care doreste sa o acceseze

Selecteaza metoda de autentificare

Conexiune SSL mutuala direct de pe echipamentul mobil. In acest caz atat clientul cat si serverul prezinta

propriul certificat digital si se stabileste conexiunea conform protocolului SSL.

Acces de pe calculator utilizand echipamentul mobil pentru autentificare. In acest caz, pentru realizarea

conexiuni SSL serverul prezinta certificatul digital iar autentificarea se realizeaza urmand pasii urmatori:

a.i. Serverul codeaza informatii privind sesiunea de lucru, intr-un format standardizat pe care il afiseaza pe ecranul calculatorului. Formatul va fi semnat de catre server folosind in acest sens certificatul sau digital

a.ii. Utilizatorul scaneaza codul respectiv folosind camera echipamentului mobil (telefon inteligent sau tableta) si decodifica informatia semnata de catre server.

a.iii. Aplicatia existenta pe telefonul mobil verifica faptul ca semnatura serverului este legitima. In caz contrar, sesiunea de autentificare nu se realizeaza.

a.iv. Utilizatorul foloseste echipamentul mobil si certificatul digital aflat pe un dispozitiv criptografic conectat la echipamentul mobil sau un certificat stocat pe echipamentul mobil in format PKCS#12 pentru a transmite catre server datele privind sesiunea si

elementele sale de identitate. Informatiile transmise vor fi semnate electronic cu certificatul digital al utilizatorului.

a.v. Serverul verifica informatiile primite, valideaza starea certificatului utilizat pentru semnare prin protocol OCSP conform RFC 2560 si daca toate informatiile sunt corecte permite accesul utilizatorului de pe calculator la serviciul solicitat

Toate certificatele digitale utilizate in sistem trebuie sa respecte standardul X509v3.
Echipamentele mobile utilizate pentru acces la informatii si pentru realizarea fluxului de autentificare care utilizeaza cod standardizat trebuie sa suporte minim sistemele de operare iOS si Android. Trebuie sa poata fi utilizate cel putin doua tipuri de dispozitive criptografice din cele enumerate mai jos pe care sa se stocheze certificatele digitale ale utilizatorului si care sa fie conectate la echipamentul mobil:
Smart card cu interfata PKCS#11 cu contact, conectat prin intermediul unui cititor

Smart card conectat prin tehnologie fara fir, de exemplu smart card NFC.

Secure SD card cu functionalitati criptografice, conectat la slotul SD card al echipamentului mobil.

De asemenea, pentru securitate sporita, cel putin unul din dispozitivele de tip smartcard utilizate trebuie sa fie certificat in conformitate cu standardul FIPS 140.2 Nivel 2.
In vederea emiterii de certificate digitale pe dispozitive mobile intr-un mod sigur, utilizatorul trebuie sa aiba la dispozitie o aplicatie de generare a certificatului digital direct pe dispozitivul mobil care sa aiba urmatoarelele functionalitati:
Sa se integreze cu autoritatea de certificare oferita. Integrarea va fi realizata prin urmatoarele elemente:

Adresa autoritatii de certificare care va emite certificatul digital.

Un cod pus la dispozitie de autoritatea de certificare in vederea emiterii certificatului digital.

Sa realizeze si sa transmita catre autoritatea de certificare, cererea PKCS#10 necesara in vederea emiterii certificatului digital

Perechea de chei (publica/privata) vor fi generate:

Software, direct pe dispozitivul mobil

Pe un dispozitiv criptografic de tip smartcard, conectat la dispozitivul mobil

Sa realizeze scrierea certificatului digital atat pe dispozitivul mobil cat si pe dispozitivul criptografic de tip smartcard conectat la acesta.

In vederea integrarii cu solutia de autentificare existenta ofertantul va pune la dispozitie un SDK precum si codul sursa al aplicatiei. Se va prezenta, de asemenea, o declaratie din partea producatorului aplicatiei care sa garanteze integrarea cu solutia de autentificare existenta.
Pentru indeplinirea cerintelor de inalta disponibilitate solutia trebuie sa permita instalarea serviciului intr-o arhitectura ce suporta failover.
Sistemul trebuie sa permita realizarea tuturor scenariilor de autentificare iar ofertantul trebuie sa demonstreze implementarea tuturor componentelor intr-un sistem informatic implementat la cel putin un client si pentru un numar de minim 450 de utilizatori.
Interfata aplicatiilor existente pe dispozitivele mobile va trebui sa fie minim in limbile romana si engleza. In acest sens se vor prezenta capturi de ecran ale aplicatiei si manuale de utilizare.
Se va urmari ca solutia pentru dispozitive mobile sa fie una matura si in acest sens se vor prezenta manuale de utilizare si capturi de ecran care sa demonstreze cerintele mai sus mentionate. De asemenea, se va organiza si o sesiune demonstrativa in care se vor prezenta functionalitatile mai sus mentionate.
Ofertantul va asigura servicii de instruire „in regim train the trainers” pentru utilizarea si administrarea aplicatiei. Instruirea va fi realizata de instructor acreditat/certificat de producatorul aplicatiei. Ofertantul va prezenta un angajament de la producatorul aplicatiei ca asigura suport tehnic on-site Beneficiarului pe toata perioada contractului, inclusiv in perioada de garantie.

3.3 Cerinte de securitate a sistemului

Aplicatia trebuie sa fie protejata impotriva incercarilor deliberate sau accidentale de acces neautorizat la datele pe care aceasta le gestioneaza. Designul solutiei de securitate trebuie sa fie astfel conceput incat sa asigure securitatea si confidentialitatea atat a datelor personale ale utilizatorilor, dar si a continutului si a anumitor functionalitati ale aplicatiei, astfel incat utilizatorii sa acceseze doar acele sectiuni si continut care le este permis prin apartenenta la un profil sau machete de securitate.

- Solutia de securitate va fi astfel configurata, incat sa nu permita persoanelor neautorizate modificarea sau alterarea semantica a informatiilor din sistem.
- Solutia de securitate va asigura consistenta datelor si va permite identificarea sursei datelor initiale si a persoanelor care au accesat sau au inregistrat aceste date in sistem.
- Solutia de securitate va asigura securizarea / protectia datelor vehiculate in sistem pe mai multe niveluri – la nivel de acces in retea, la nivel de aplicatie si la nivel de baza de date.
- Nu se permite acces neautentificat la date si informatii (mai putin zona publica a aplicatiei). Orice acces in aplicatie (atat la nivelul utilizatorilor cat si la nivelul altor module de aplicatie) este precedat de identificarea, autentificarea si autorizarea accesului ;
- Parolele utilizatorilor trebuie stocate criptat in baza de date folosind algoritmul criptografic SHA512;
- Parolele de acces intre modulele aplicatiei (de ex la baza de date) trebuie sa fie stocate criptat in fisierele de configurare ale aplicatiei;
- Credentialele de acces (username, parola) nu se transmit in clar prin retea la autentificarea utilizatorilor sau intre modulele aplicatiei;
- Sesiunile de lucru inactive ale utilizatorilor trebuie sa expire dupa o perioada de timp configurabila (implicit 10 minute);
- Serviciile si porturile de comunicatie folosite vor fi documentate intr-o lista a serviciilor utilizate. Serviciile si porturile neutilizate vor fi dezactivate;
- Aplicatia va fi instalata si configurata numai pe sisteme care au aplicate ultimele patch-uri de securitate;

3.3.1 Testare de securitate

Serviciile de evaluare a securitatii sistemului informatic vor adresa aplicatiile, sistemul informatic asociat acestora, echipamentele pe care se bazeaza aceste aplicatii si interfetele cu alte sisteme informatice si aplicatii specifice.
Obiectivul testelor de securitate este identificarea vulnerabilitatilor specifice ale sistemului informatic prin evaluari de securitate in baza standardelor internationale (ex ISO 27001) si a celor mai bune practici in domeniul securitatii informatiei, avand in vedere designul, implementarea, utilizarea, mentenanta si dezvoltarea sistemului.
In cadrul evaluarilor vor fi realizate inclusiv teste de penetrare („ethical hacking”) din interiorul retelei.
Ofertantii vor realiza urmatorele analize:
Conformitatea solutiei cu cerintele de securitate din cadrul proiectului;

Evaluarea securitatii din perspectiva modului de implementare si configurare a sistemului informatic. Vor fi analizate din punct de vedere al securitatii informatiei toate componentele sistemului informatic: aplicatii, baze de date si infrastructura IT.

Verificarea si validarea modului de implementare a controalelor de securitate;

Teste de securitate de tip “ethical hacking” asupra intregului sistemului;

Analiza de risc a sistemului in urma vulnerabilitatilor identificate.

Oferta va mentiona metodologiile si tehnicile utilizate in evaluarea vulnerabilitatilor (ca de ex. National Institute of Standards and Technology – NIST, Open Source Security Testing Methodology – OSSTM, Open Information Systems Security Group - OISSG, Information Systems Audit and Control Association – ISACA, etc).
In urma executarii acestei activitati se va livra un raport ce va contine informatii detaliate privind vulnerabilitatile identificate si masuri si sugestii de remediere a acestora.
Structural, raportul va cuprinde :

Obiectivele si scopul evaluarii

Prezentare succinta a metodologiei utilizate

Descrierea contextului in care s-a desfasurat evaluarea

Recomandari tehnice pentru remedierea vulnerabilitatilor

Prezentarea individuala a vulnerabilitatilor descoperite dupa cum urmeaza:

descrierea vulnerabilitatii

catalogarea vulnerabilitatii

descrierea tehnica

analiza severitatii si probabilitatii

contramasuri recomandate pentru remediere

Alte detalii si recomandari

Anexa cu lista testelor de securitate efectuate

Informatiile prezente in raport vor contine, printre altele :
Detalii despre reteaua si sistemele evaluate :

Host-urile si serviciile active (adrese IP, porturi deschise, inchise, filtrate)

Tipul, versiunea, nivelul de patching al aplicatiilor

Sistemul de operare

Lista vulnerabilitatilor descoperite clasificata conform cu severitatea vulnerabilitatilor excluzand falsele pozitive.

Detalierea metodelor si actiunilor utilizate in exploatarea vulnerabilitatilor.

Lista de recomandari pentru remedierea vulnerabilitatilor.

In carul ofertei tehnice, ofertantii trebuie sa prezinte un plan de testare de securitate care sa sumarizeze testele propuse pentru etapa de testare la punerea in productie a sistemului.

3.3.2 Infrastructura de securitate informatica

Infrastructura de securitate informatica implementata va asigura mecanismele necesare schimbului protejat de informatii. In acest sens se va asigura implementarea urmatoarelor componente:
Infrastructura de chei publice (PKI – Public Key Infrastructure) pentru gestiunea certificatelor digitale de semnatura electronica criptare si autentificare – se vor oferi licente pentru un numar nelimitat de utilizatori – cu urmatoarele componente:

Modul de gestiune a certificatelor digitale;

Modul de validare online a starii certificatului;

Modul de marcare temporala;

Modul de recuperare a cheilor private de criptare;

Modul de administrare a dispozitivelor criptografice ale utilizatorilor

Accesul la sistem utilizand autentificare de pe terminale mobile

Software pentru validarea documentelor semnate electronic și a mărcii temporale

Software pentru semnarea automatizată a documentelor electronice

Dispozitive criptografice

Implementarea infrastructurii de securitate trebuie sa asigure migrarea si integrarea cu componentele utilizate in acest moment, astfel:
se va realiza migrarea de la infrastructura PKI existenta pentu a se asigura continuitatea serviciilor asociate certificatelor digitale emise;

se va asigura integrarea cu solutia de autentificare existenta pentru a se permite accesul la sistem utilizand autentificare de pe terminale mobile.

Sistem de securitate impotriva atacurilor informatice

Pentru protejarea solutiei propuse la nivel logic de atacuri informatice atat din exterior cat si din interior, aceasta va fi prevazuta cu un sistem de securitate care sa corespunda urmatoarelor cerinte:
Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete cu header IP incorect

Sistemul trebuie sa fie capabil sa identifice si sa blocheze fragmente IP invalide si pachete cu fragmente IP duplicate

Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete fragmentate cu lungimea mai mare de 65535 octeti

Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete cu checksum IP, TCP si UDP invalid

Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete ce au lungimea mai mica decat cea specificata in header-ul lor IP

Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete de tipul ICMP ce sunt prea scurte pentru a contine un header ICMP valid

Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete TCP cu o combinatie invalida de flag-uri TCP

Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete in baza unor filtre configurate de utilizator la nivel 3 sau la nivel 4 al stivei OSI

Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete ce sunt transmise cu o frecventa mai mare decat limita configurata de utilzator

Sistemul trebuie sa fie capabil sa limiteze frecventa pachetelor UDP si ICMP in baza valorilor configurate de utilizator

Sistemul trebuie sa fie capabil sa identifice si sa blocheze atacuri bazate pe transmiterea unui numar mai mare de pachete de tipul TCP SYN decat o limita configurata

Sistemul trebuie sa fie capabil sa identifice si sa blocheze atacuri bazate pe transmiterea unui numar mai mare de pachete TCP SYN decat pachete TCP ACK

Sistemul trebuie sa fie capabil sa identifice si sa blocheze atacuri de tipul TCP SYN Flood de la adrese falsificate.

Sistemul trebuie sa fie capabil sa limiteze numarul maxim de conexiuni TCP concurente de la o singura sursa

Sistemul trebuie sa fie capabil sa limiteze volumul total de trafic specific unei expresii de nivel 3 sau nivel 4 al stivei OSI in baza unei valori configurate

Sistemul trebuie sa fie capabil sa identifice si sa blocheze traficul in baza unei clasificari de geolocatie.

Sistemul trebuie sa permita configurarea de liste statice cu IP-uri blocate si IP-uri legitime

Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete ce contin solicitari HTTP invalide

Sistemul trebuie sa fie capabil sa identifice si sa blocheze atacuri bazate pe transmiterea de solicitari HTTP cu o frecventa mai mare decat cea configurata

Sistemul trebuie sa permita verificarea surselor solicitarilor HTTP prin mecanisme de redirectionare HTTP

Sistemul trebuie sa permita finalizarea solicitarilor HTTP in cazul in care header-ul HTTP nu este transmis in totalitate intr-un interval de 60 de secunde

Sistemul trebuie sa fie capabil sa identifice si sa blocheze atacuri de tipul DNS Request Flood de la adrese falsificate

Sistemul trebuie sa permita blocarea solicitarilor DNS in baza unor reguli specificate de utilizator

Sistemul trebuie sa fie capabil sa identifice si sa blocheze pachete cu solicitari SSL/TLS invalide

Sistemul trebuie sa fie capabil sa identifice si sa blocheze mesaje SIP invalide

Sistemul trebuie sa fie capabil sa identifice si sa blocheze atacuri bazate pe transmiterea de mesaje SIP cu o frecventa mai mare decat cea configurata

Sistemul trebuie sa fie capabil sa identifice in baza de semnaturi actualizate in timp real atacuri de tip malware (cel putin BlackEnergy slowloris, LOIC, darknes, Yoyo DDOS,)

Sistemul trebuie sa fie capabil sa ofere notificari SMTP si Syslog cu privire la starea sitemului si la adresele IP blocate

Sistemul trebuie sa permita autentificarea si autorizarea utilizatorilor folosind baza de date locala, RADIUS sau TACACS

Sistemul trebuie sa permita efecturea operatiunilor de back-up si restaurare utilizand un server dedicat. Comunicatia cu acest server se va realiza utilizand un protocol criptat

Sistemul trebuie sa fie transparent la tag-uri 802.1Q si la pachete de tipul STP BPDU

Sistemul trebuie sa fie capabil de hardware bypass in caz de oprire a alimentarii si de software bypass in caz de efectuare a operatiunilor de mentenanta la nivelul sistemului de operare

Sistemul trebuie sa permita propagarea starii link-ului catre perechea protejata. Propagarea starii trebuie sa fie configurabila.

Sistemul nu trebuie sa intrerupa fluxul de trafic atunci cand se modifica nivelul protectie.

Sistemul trebuie sa asigura protectia pentru un trafic cumulat (input si output) de 2 Gbps

Sistemul trebuie sa fie capabil sa identifice atacuri de tip DoS/DDoS in trafic criptat SSL

Sistemul trebuie sa fie capabil sa redirectioneze traficul protejat atat automat, in baza unei limite de trafic predefinite, cat si manual catre o zona de procesare date (in cloud) aflata sub controlul producatorului care sa permita curatirea traficului de atacuri de tipul DoS/DDoS. Sistemul va folosi, ca si mecanisme de interconectare cu solutia in-cloud, redirectarea DNS sau rutarea BGP.

3.4 Managementul utilizatorilor si accesul la sistem

Pentru securizarea sistemului informatic trebuie utilizat un modul de securitate dedicat, ce va contine ansamblul mecanismelor de securitate oferite. Prin mecanisme de securitate se intelege totalitatea masurilor si actiunilor ce sunt aplicate in cadrul unui sistem pentru a asigura buna functionare a acestuia (rezistenta la atacuri). Deasemenea, trebuie sa asigure ca informatiile vehiculate prin sistem nu pot fi alterate de terte parti.
Se identifica urmatoarele categorii principale de capabilitati:

- Administrare utilizatori
- Autentificare
- Asigurarea accesului la resurse
- Trasarea actiunilor in cadrul sistemului

3.4.1 Administrare utilizatori

Functionalitatile de administrare trebuie expuse la nivel de Back Office ca o interfata distincta, acestea urmand sa permita:

a) Definirea/modificarea/stergerea de utilizatori

b) Asocierea de roluri utilizatorilor (roluri ce vor stabili nivelul lor de acces in sistem)

c) Vizualizarea logurilor de activitate ale utilizatorilor

3.4.2 Mecanisme de autentificare

Autentificarea utilizatorilor in cadrul sistemului trebuie sa poata fi realiza pe baza de certificat digital, username si parola sau certificat digital organizational, username si parola. Indiferent de metoda de autentificare se va folosi comunicarea pe canale securizate pe baza protocolului SSL. In cazul folosirii certificatelor digitale acestea sunt mapate cu un utilizator al sistemului, acesta neavand nevoie de username si parola. Pentru autentificare bazata pe username si parola nu este nevoie ca utilizatorul sa fie in posesia unui certificat digital pentru a accesa sistemul. Autentificarea cu certificat digital organizational, username si parola presupune indentificarea entitatii pe baza certificatului digital si identificarea unui utilizator al entitatii pe baza perechii nume utilizator si parola. Mecanismul de autentificare este un unul generic si configurabil permitand comutarea rapida intre cele 3 modalitati de autentificare.

3.4.3 Asigurarea accesului la resurse

Prin verificare dreptului de acces la resurse se intelege multimea de operatii ce trebuie realizata pentru verificarea rolurilor, drepturilor si competentelor pe care un utilizator le are in cadrul aplicatiei.
Modelul de autorizare folosit trebuie sa fie unul flexibil, bazat pe roluri (Role Based Access Control), facilitand gestiunea utilizatorilor si alocarea acestora conform drepturilor pe care le au in operarea sistemului.
La nivel programatic sunt definite, cu un grad de granularitate ridicat, rolurile de baza ale sistemului si se stabileste legatura dintre roluri si meniurile aplicatiei. Administratorul sistemului are la dispozitie o interfata facila pentru a compune noi roluri din cele de baza. Tot la nivel programatic se stabilesc actiunile pe care un rol le poate indeplinii. Sistemul ofera astfel doua mecanisme de verificare si protectie importiva accesului neautorizat asupra unei resurse:

- Verificare proactiva – la autentificare sistemul incarca pentru fiecare utilizator rolul asociat si compune meniul la care acesta are acces. Se stabileste astfel aria de competente a utilizatorului logat.
- Verificare reactiva – se refera le verificare drepturilor pe care un utilizator (reprezentat prin rolul asociat) le are asupra resurselor din sistem. Acest tip de verificare se realizeaza pentru fiecare operatiune realizata in sistem si impiedica un utilizator autentificat sa obtina acces asupra unor resurse la care nu are acces.

3.4.4 Trasabilitatea actiunilor in cadrul sistemului

Actiunile desfasurate de catre un utilizator in cadrul sistemului sunt inregistrate pentru a oferi o imagine clara asupra fluxurilor sistemului. Aceste informatii trebuie sa fie pastrate intr-o zona sigura diferita fata de zona de persistenta a datelor pentru a nu permite alterarea lor de catre operatorul sistemului. Prin analiza logurilor se pot extrage informatii utile despre modalitatea de folosire a sistemului sau eventualele erori ce pot aparea in cadrul sistemului. Logurile pot fi consultate de catre administratorii sistemului insa nu pot fi modificate. Logurile pot fi

puse la dispozitia unor institutii abilitate sa auditeze sisteme electronice pentru a demonstra ca sistemul se comporta conform asteptarilor.

3.4.5 Accesul administratorilor de sistem

Tinand cont de faptul ca sistemul vehiculeaza date de interes national, inclusiv accesul local administratorilor sistemului de la statiile de administrare si monitorizare trebuie gestionat intr-un mod cat mai sigur astfel incat sa nu poata exista incidente de securitate. Astfel pe langa mecanismele de securitate si autentificare la nivelul aplicatiilor sistemului, va fi reglementat si accesul administratorilor si personalului tehnic care prin accesul la statiile de administrare si monitorizare gestioneaza resursele acestuia si asigura buna functionare, monitorizare si raportare.
In acest sens, la nivelul sistemul pentru fiecare statie de administrare si monitorizare se va prevedea un cititor de carduri cu urmatoarele caracteristici:
Standarde de functionare:

Trebuie sa fie conforma cu standardele majore in domeniu cum ar fi FIPS 201, ISO 7816, EMV 2000, Microsoft

WHQL, USB CCID, PC / SC, HBCI, PC-2001.

Trebuie sa fie compatibila cu standardele USB 1.1 si USB 2.0.

Trebuie sa fie compatibile cu standararde PCKS 11 si Microsoft CSP

Suport Hardware si Software:

Trebuie sa aiba suport pentru sistemele de operare de tip Windows, Linux,

Trebuie sa aiba suport atat pentru pentru echipamente mobile, cat si statii de lucru si servere.

Trebuie sa functioneze fara sursa de alimentare separata.

Suport smartcard-uri:

Trebuie sa suporte smartcard-uri de tip ISO 7816 clasa A, B si C de 1.8V, 3V si 5V

Trebuie sa suporte smartcard-uri de format ID-1

Trebuie sa suporte protocoalele T=0, T=1

Trebuie sa beneficieze de suport pentru detectia tipului de card;

Trebuie sa suporte smartcard-uri al caror ceas functioneaza pana la o frecventa de 8 Mhz;

Inserarea smartcard-urilor trebuie sa poata fi realizata orizontal sau vertical.

Solutia trebuie sa permita identificarea usoara a statusului de functionare prin avertizare luminoasa;

Solutia trebuie sa beneficieze de suport pentru detectia miscarii si pentru oprire automata in caz de nefolosire;

Mediu de functionare:

Trebuie sa beneficieze de protectie la scurt-circuit si supraincalzire

Trebuie sa asigure cel putin 100,000 utilizari

In acest sens, se vor prevedea carduri de acces tip SmartCard pentru toti administratorii sistemului si personalul tehnic implicat in procesele de configurare, monitorizare si raportare cu care se vor autentifica pe statiile de administrare si monitorizare. Cardurile vor avea urmatoarele caracteristici minimale:
Standarde suportate: ISO/IEC 7810, 7816

Cip smartcard certificat Common Criteria EAL 5+

Integreaza in cip un procesor de inalta performanta pentru operatiunile criptografice cu chei simetrice si asimetrice

Disponibile si cu tehnici de anti-piratare, cum ar fi holograme, folie holografica, OVI (Optical Variable Ink)

Preincarcate cu un profil electric care suporta 9 key PKI cu marimi configurabile precum si certificate X.509

Suporta una sau mai multe tehnologii de proximitate (contactless) cum ar fi: iCLASS 32k, NXP MIFARE, DEXFire EV1.

Suporta specificatiile JavaCard 2.2.2 si Global 2.1.1

Functionaza cu cititoarele compatibile PC/SC

Viteza citire: 230.4 kbps la 3.57 Mhz in modul de contact si 106-848 kbps in modul de proximitate (in functie de tehnologii)

Memorie EEPROM: 80KB

Cicluri de rescriere: 500.000

Retentie date EEPROM: 20 ani

Masuri de securitate: senzori frecventa ceas, temperatura, voltaj si lumina; detectia atacurilor de tip Single Fault Injection (SFI) precum si protectie impotriva atacurilor SPA/DPA si DFA.

Middelware pentru carduri:

1. sa ofere suport serviciilor PKI
2. sa suporte tehnologia “java card”
3. trebuie sa permita blocarea sau delogarea utilizatorului de la statia de lucru cand smartcardul a fost indepartat

3.5 Confidentialitatea datelor

Securitatea mediului de comunicare trebuie asigurata prin folosirea protocolului HTTPS (bazat pe SSL 128 biti). Pentru a permite acest tip de comunicare serverul trebuie sa dispuna de un certificat digital utilizabil pentru criptare si semnare. Folosirea acestui protocol asigura criptarea comunicatiei intre cele doua entitati aflate in discutie facand imposibila intelegerea mesajelor schimbate intre entitati.
Toate informatiile sensibile care trebuie salvate in cadrul sistemului informatic vor fi mai intai criptate sau tinute sub forma de hash. Exemplu de informatii care trebuiesc tinute criptat sunt string-urile de conectare la baze de date daca acestea contin acreditive pentru conectare iar parolele utilizatorilor sunt date care trebuie salvate.
Sistemul trebuie sa asigure urmatoarele functionalitati la nivel de securitate si confidentialitatea datelor:
Sistemul trebuie protejat impotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acestea le inmagazineaza.

Sistemul va avea un sistem de securitate care permite protejarea informaţiei, atat fata de accesul neautorizat intern, cat si fata de accesul neautorizat extern.

Sistemul va indeplini anumite cerinţe din punct de vedere al securitatii, cum ar fi autentificarea unica a utilizatorilor si autorizarea acestora in sistem prin mecanisme de tip autentificare unica prin intermediul rolurilor si privilegiilor.

Utilizatorii vor avea acces numai la aplicaţiile si documentele pentru care au drepturi.

Sistemul va fi proiectat si implementat din punct de vedere al securitatii pe baza legilor, regulamentelor si instrucţiunilor in vigoare privind securitatea, confidenţialitatea si protectia datelor.

Sistemul va fi proiectat astfel incat sa nu aiba porturi deschise către exterior (altele decât cele necesare bunei funcţionari a sistemului) si sa ofere mecanisme de control al accesului prin implementarea politicilor de securitate multilevel conform necesitatii de interconectare.

Vor fi asigurate mecanisme de securitate implementate pe mai multe niveluri, la nivel de prezentare, aplicaţie si la nivel de baza de date si se vor permite autentificarea, identificarea, verificarea drepturilor si permisiunilor, supravegherea cererilor de servicii si operaţiilor executate de persoana care a generat, a modificat sau a sters o informaţie.

Pentru asigurarea securitatii datelor trasportate componentele funcţionale ale sistemului vor trebui sa asigure instrumente native pentru conectarea si trasportul de date către baza de date pe canale criptate utilizând standarde de tip SSL.

Utilizatorul final nu va avea acces la baza de date decât prin intermediul aplicaţiei.

Comunicaţia clienţilor cu sistemul SICAP trebuie sa fie garantata din punct de vedere al confidentialitatii in orice moment de timp. Pentru comunicaţia online este obligatoriu sa se asigure conexiune de tip HTTPS (SSL 128 biti).

Transmisiile de credentiale (username si parola) intre modulele aplicatiei sau cu alte aplicatii prin flux-urile de date definite se realizeaza numai in mod criptat (SSL v3)

Utilizatorii cu drepturi administrative vor accesa interfata aplicatiei folosind un canal securizat end-to-end (HTTPS)

Certificatul SSL la nivel de server web va fi emis de o autoritate publica recunoscuta de certificare ;

Validarea tuturor datelor de intrare transmise de client inainte de procesarea lor, incluzand toti parametrii, adrese URL, headere HTTP (de ex. Cookie, User Agent):

Validarea tipului de date: (integer, alpha, alnum ,digit, etc.);

Sintaxa corecta (regexp);

Limita de lungime ;

Filtrarea caracterelor special precum: < > " ' % ( ) & + \ \' \" ;

Utilizarea de "Stored precedures" si/sau "Prepared statemens" pentru interogarile SQL;

Aplicatia nu va pastra informatii reziduale (fisiere temporare, copii de siguranta, etc.) care ar putea fi accesate prin interfata web;

In vederea asigurarii confidentialitatii datelor solutia propusa trebuie sa aiba in componenta un sistem care sa asigure:

- criptarea datelor critice din bazele de date
- auditul activitatilor desfasurate in bazele de date
- scanarea si monitorizarea vulnerabilitatilor la nivelul bazelor de date.

In acest sens, sistemul propus trebuie sa aiba urmatoarele caracteristici:
Sistemul trebuie sa se prezinta ca o platforma unitara si integrata;

Sistemul trebuie sa poata cripta datele atat la nivelul bazelor de date cat si la nivelul sistemelor de fisiere;

Sistemul trebuie sa fie transparent din punct de vedere al aplicatiilor;

Sistemul trebuie sa prezinte o consola centralizata de management din care sa se poata executa, monitoriza su audita toate activitatile;

Sistemul trebuie sa prezinte facilitati de administrare si audit al cheilor de criptare cat si al politicilor de criptare implementate din consola de management unica;

Sistemul trebuie sa suporte criptare pe sisteme de operare UNIX, Linux si Windows;

Sistemul trebuie sa suporte criptare pe baze de date de tip Oracle, DB2, MS SQL, Sybase si MySQL;

Sistemul trebuie sa gestioneze obiectele criptate la nivel de agenti iar acestia sa poata sa verifice orice incercare de acces a datelor si in baza politicilor definite sa permita sau nu accesul;

Sistemul trebuie sa permita o separare a activitatilor astfel incat sa se execute criptarea fisierelor fara a actiona asupra metadatelor;

Sistemul trebuie sa permita implementarea transparenta a politicilor de criptare la nivelul bazelor de date fara a modifica arhitectura acestora;

Sistemul trebuie sa poata implementa politicile de criptare a datelor cu un impact minim la nivelul aplicatiilor prin identificarea la nivel de bloc a segmentelor de date folosite;

Sistemul trebuie sa permita definirea de roluri distincte la nivel de administrare astfel incat sa poata exista un administrator al cheilor de criptare si un altul sa poata administra politicile implementate cu aceste chei;

Sistemul trebuie sa suporte mecanisme de inalta disponibilitate care sa permita realizarea de sisteme cluster cu balansare atat la nivel local cat si in distributie geografica;

Sistemul trebuie sa poata genera log-uri de audit ce pot fi colectate intro componenta de tip SIEM (Security information and event management);

Sistemul trebuie sa inregistreze informatii audit pentru toate activitatile executate la nivelul bazelor de date;

Sistemul trebuie sa ofere funcţii de audit pentru acces şi folosire indicând autorul, modificarea care a fost făcuta (atunci când este posibil), data şi ora la care elementele au fost create, modificate, vizualizate, extrase sau şterse. Trebuie sa fie posibila generarea unor rapoarte de audit bazate pe aceste date;

Solutia propusa trebuie sa protejeze sistemul SICAP impotriva pierderilor, modificarilor si distrugerii datelor la nivelul bazei de date in care sunt tinute informatiile de interes national;

Solutia propusa trebuie sa asigure mijloacele pentru monitorizarea continua a accesului la baze de date critice, prevenind accesul sau schimbari neautorizare asupra datelor acestora;

Sistemul trebuie sa poate declansa masuri preventive in timp real atunci cand sunt identificate tranzactii suspecte. Informatiile privitoare la tranzactii sunt stocate intr-un mediu centralizat si securizat, in scopuri de audit.

Sistemul trebuie sa permita scanarea infrastructurii de baze de date in vederea detectarii de vulnerabilitati si a prezentarii unui raport catre administratori cu propuneri de remediere a acestora;

Sistemul trebuie sa poata detecta vulnerabilitati la nivelul bazelor de date de tipul: pachete lipsa, parole slabe, acces si modificari ale datelor neautorizate, update-uri critice, drepturi de acces configurate in mod necorespunzator;

Sistemul trebuie sa poata descoperi si clasifica datele la nivelul bazelor de date; sistemul trebuie sa aiba suport pentru Oracle, DB2, Sybase, Microsoft SQL Server, Informix,mySQL, Teradata, siPostgreSQL;

Solutia de criptare, audit si scanare vulnerabilitati va fi integrata si folosita la nivelul mediul de productie.

4. DESCRIEREA TEHNICA A PROIECTULUI

4.1 Arhitectura functionala a sistemului

Arhitectura functionala a sistemului este prezentata in schema de mai jos:

Arhitectura sistemului informatic trebuie să asigure:

- Accesul facil al utilizatorilor la informatiile si operatiile ce le sunt puse la dispozitie;
- Viteză mare de acces la informaţii şi posibilităţi avansate de regăsire a informaţiei pentru maxim de claritate si relevanta;
- Securitatea informaţiilor şi a accesului la informaţii pe bază de drepturi şi parole;
- Informatizarea sistemelor informaţionale decizionale şi a proceselor existente;
- Implementarea de modele, algoritmi şi metode statistice, pentru alocarea optimă a resurselor;
- Asigurarea unui management modern prin perfecţionarea continuă a tehnicilor manageriale, având ca suport sistemul informaţional şi informatic al instituţiei;
- Transformarea software-ului dintr-un element de cost într-o achiziţie strategică;
- Eficientizarea activităţii şi utilizarea performantă a infrastructurii hardware.

Sistemul informatic va trebui să răspundă urmatarelor cerinte:

- **Flexibilitatea**, exemplificată prin capacitatea aplicaţiei de a lucra cu reguli de tranzacţionare stabilite sau modificabile de către utilizator;
- **Modularitatea,** care implică dezvoltarea aplicaţiei în jurul unui nucleu căruia i se pot adăuga module şi proceduri noi pentru un upgrade uşor, având o arhitectură deschisă care sa permită integrarea cu alte aplicaţii sau dezvoltarea ulterioară de noi funcţii şi integrarea completă a acestora;
- **Interfaţa modernă, intuitiva şi personalizabilă,** având sectiuni configurabile şi asigurând adaptarea la necesităţi de design practic, fiecare utilizator putându-şi particulariza aplicaţia pentru genul de muncă pe care îl efectuează;
- **Modalitatea de căutare sa fie naturală, în timp real, senzitivă** şi să se facă după criterii de căutare definite de utilizator;
- **Separarea logica a operaţiilor între serverul de gestiune a bazei de date şi aplicaţia client,** prin realizarea operaţiilor de calcul in cadrul aplicaţiei de client şi folosirea serverului de baze de date pentru tranzacţionare şi relaţionare. În acest mod se separa logic operaţiile efectuate între serverul de baze de date şi aplicaţia client;
- **Sa aibă nivel ridicat de securitate a datelor şi tranzacţiilor,** utilizatorii să fie definiţi ca aparţinând unui grup, iar drepturile să se dea fie pe grup, fie pe utilizator explicit, existând două nivele de protecţie a informaţiei: al bazei de date şi mecanism intern de protecţie.

Sistemul informatic propus trebuie sa garanteze functionare permanenta a serviciilor asigurate de catre AADR in domeniul achizitiilor publice, prin functionare in paralel a sistemelor informatice existente.

4.2 Arhitectura sistemului informatic si de comunicatii

Sistemul informatic central va fi proiectat astfel încât să funcţioneze în regim de înaltă performanţă şi disponibilitate şi va fi separat pe trei niveluri, conform celor mai bune în domeniu: stocarea datelor, prelucrare şi prezentare.

Proiectarea sistemului se va face astfel incat sa respecte recomandarile de performanta si securitate in domeniu. Astfel, sistemul va fi de tip “no single point of failure” cu componente redundante atat la nivel aplicativ cat si la nivel hardware.

Sistemul astfel proiectat va prezenta 3 zone distince:

- ***Nivel de prezentare***: este compus din servere web de prezentare si acces la serviciile sistemului. Acest nivel va fi balansat la nivelul cererilor din exteriorul sistemul printro componenta dedicata instalata si integrata in platforma de comunicatii.
- **Nivel de aplicatie**: este compus din servere de aplicatii ce gestioneaza modulele software ce vor fi instalar
- **Nivel baze de date**: trebuie sa fie constituit din servere de baza de date configurate in cluster mod activ activ care sa asigure balansarea incarcarii, precum si scalabilitate si disponibilitate maxima, pe care ruleaza sistemul de gestiune a bazei de date.

Zonele trebuie sa fie delimitate la nivel logic si separate prin intermediul functionalitatilor de tip firewall. Accesul dintro zona in alta trebuie sa se faca controlat si numai pentru resursele care necesita acest lucru. Accesul utilizatorilor se va permite doar la nivelul de prezentare, iar cererile catre nivelul aplicativ vor gestionate de acesta. Utilizatorii nu trebuie sa aiba acces sub nici o forma catre nivelul bazelor de date.
In dezvoltarea sistemului va trebui sa se tina cont de numărul mare de utilizatori si de volumul mare de date si documente care vor fi stocate in vederea asigurarii accesului ulterior de către institutiile cu drept de acces.
In acest sens componentele functionale ale sistemului vor fi:

- Portal (cu servere web si reverse proxy in DMZ)
- Platforma de aplicatii
- Sistem de gestiune baze de date
- Platforma de analiza si raportare
- Platforma management securizat al cererilor si solicitarilor din partea utilizatorilor
- Platforma pentru instruirea utilizatorilor si lucru colaborativ
- Platforma de manegement infrastructura de chei publice
- Platforma validarea documentelor semnate electronic și a mărcii temporale
- Platforma pentru semnarea automatizată a documentelor electronice
- Monitorizare
- Backup
- Management si suport

In acest sens ofertantul va propune o arhitectura functionala care sa respecte prevederile caietului de sarcini, in care va evidentia componentele propuse, modul de instalare a acestora, resursele alocate si mecanismele de inalta disponiblitate, redundanta, scalabilitate si flexibilitate.
Oferta tehnica va contine un tabel si o reprezentare grafica a sistemului din care sa reiasa toate masinile ce vor rula in cadrul sistemului, funtionalitatea lor, resursele de processor si memorie alocate, software de baza instalat si versiunea, cat si apartenenta de nivel in cadrul sistemului.
Componentele hardware ale sistemului vor fi instalate si configurare redundant, intr-o arhitectura de tip “no single point of failure”. Toate conexiunile de tip Ethernet, FibreChannel etc vor fi proiectate si instalate redundant. Ofertantii vor propune arhitecturi de tip cluster atat la nivelul de baza cat si la nivel aplicativ.

Platforma de testare

Pentru testarea si dezvoltarea functionalitatilor sistemului se va utiliza o platforma dedicata de testare care include toate componentele functionale din cadrul platformei de productie. Platforma de testare va folosi resurse de procesare dedicate fata de platforma de productie, putand folosi aceleasi resurse de stocare fara partajare de volume. Arhitectura mediului de testare va replica arhitectura mediului de productie.

4.3 Aspecte non-functionale

4.3.1 Scalabilitate

Scalabilitatea este asigurată prin:

Virtualizare – permițând adăugarea de mașini virtuale noi pe infrastructura existentă fără impact major;

Solutia de stocare asigura suport pentru cresterea capacitatii de stocare prin adaugarea de noi hard-disk-uri;

Șasiul de servere blade folosit în sistem permite adăugarea de servere de tip blade suplimentare

Pentru servere s-au prevăzut sloturi de procesor și memorie libere astfel încât să se poată adăuga ulterior cantități suplimentare pentru mărirea capabilităților hardware;

Software-ul folosit este scalabil folosind pattern-uri larg răspândite în industrie (server de aplicație scalabil, server de portal scalabil, servere de baze de date scalabil);

Pentru componentele software se folosește o arhitectură de tip cluster, aceasta permite adăugarea ulterioară a altor servere în cluster pentru mărirea performanței software.

4.3.2 Flexibilitate

Sistemul va prezinta un grad mare de parametrizare care să permită modificări rapide și facile în cadrul aplicației. Trebuie să existe flexibilitate la reconfigurarea soluției (când vor apărea modificări în cerințe) și să fie necesar cât mai puțin efort de programare pentru adaptare la specificul serviciilor.
Sistemul va fi complet configurabil și capabil să facă față necesităților unui număr crescând de utilizatori.
Sistemele informatice și rețeaua de comunicații vor folosi standarde deschise, neproprietare, pentru a permite refolosirea acestora în cazul dezvoltărilor ulterioare ale sistemului.

4.3.3 Performanță

Pentru a obține o performanță foarte bună, baza de date de producție trebuie să îndeplinească următoarele cerințe:
trebuie să scrie în mai multe fișiere pe disc simultan în timpul unei operații de salvare, în vederea creșterii performanței;

trebuie să citească din mai multe fișiere pe disc simultan în timpul unei operații de restaurare, în vederea creșterii performanței;

trebuie să permită citirea și scrierea paralelă în timpul unei operații de salvare;

trebuie să permită citirea și scrierea paralelă în timpul unei operații de restaurare;

trebuie să poată rula pe sisteme de tip cluster în mod activ-activ;

baza de date trebuie să asigure partajarea automată a încărcării intre nodurile cluster-ului în vederea măririi productivității;

să conțină propriul soft de clusterware integrat, astfel încât să permită rularea pe diferite platforme și sisteme de operare fără achiziționarea de soft de cluster adițional de la producătorul sistemului de operare;

trebuie să ofere abilitatea să partiționeze tabele în vederea creșterii performantei și administrării facile a datelor din tabele;

trebuie să permită unei tabele să fie partiționate bazându-se pe una sau mai multe valori specifice de date, așa cum este hotărât de către administratorul bazei de date;

să ofere posibilitatea de partiționare logică a tabelelor mari în scopul reducerii timpului de acces la date după diverse criterii de partiționare (listă, interval, algoritmi de rezumat sau hash) și toate combinațiile acestora (de exemplu listă - interval);

trebuie să permită definirea cantității minime de date transferate intre disc și memoria locală a bazei de date la o cerere;

trebuie să ofere facilitatea să rețină date din tabele special indicate în memoria locală pentru o perioadă

nedefinită de timp;

trebuie să permită setarea mărimii unei zone din memoria locală, rezervată să rețină date din tabele special indicate, pentru o perioadă nedefinită de timp;

trebuie să aibă un optimizator bazat pe cost pentru a optimiza interogările;

instanțe multiple, izolate, și complet funcționale ale bazei de date trebuie să poată coexista pe un singur nod fizic;

4.3.4 Uzabilitate

Sistemul va avea o interfață utilizator ușor de folosit și intuitivă în concordanță cu standardele din domeniu. Sistemul va permite navigarea facilă în și între toate modulele și accesarea tuturor funcțiilor și comenzilor la care utilizatorul are acordate drepturi în cadrul aceleiași sesiuni de lucru.

5. INFRASTRUCTURA HARDWARE

5.1 Cerinte generale privind platforma hardware

Sistemul informatic colaborativ pentru achizitii publice va rula pe o platforma hardware compusa din urmatoarele elemente prinicipale:

Echipament	**Cantitate**
Sasiu servere lamelare	1
Server de baza de date (server tip 1)	2
Servere platforma virtualizare (server tip 2)	6
Servere infrastructura securitate	6
Sistem de stocare date	1
Sistem de backup pe disc	1
Rack 19”	2
Consola TFT	1
UPS rackabil	2
Statie de lucru	1
Dispozitive criptografice	2
Platforma comunicatii IPS, firewall, switch L3	2
Echipamente Platforma Colaborativa de Instruire (set)	3
Echipamente camera tehnica (set)	1

Nota: Oferta va include toate componentele necesare asigurarii functionarii solutiei in conformitate cu toate cerintele din prezenta documentatie prin includerea tuturor livrabilelor necesare.

5.2 Platforma de procesare si stocare

5.2.1 Sasiu servere lamelare

In cadrul proiectului se va livra un sasiu de servere lamelare ce va acomoda masinile pentru baze de date cat si masinile care vor sustine mediul virtual. Acesta va asigura si modulele necesare pentru interconectarea cu sistemul de stocare si cu platforma de comunicatii.

CARACTERISTICA	**Specificatie tehnica**
Format	Maxim 10U
Sistem de ventilatie	N+1 Redundant, hot-swap
Sistem de alimentare	N+N Redundant, hot-swap, 220V 50Hz
Tip blade-uri suportate	Sasiul trebuie sa suporte intern: - servere lamelare cu procesoare in tehnologie RISC/EPIC; - servere lamelare cu procesoare in tehnologie CISC x86 ; - lame de tip storage ce pot acomoda minim 6 unitati de disk ce pot fi expuse catre serverele din sasiu
Module inteconectare	2 x switch-uri 10 Gbps 2 x switch-uri 8Gbps FibreChannel
Servere blade instalabile	Sasiul trebuie sa poata acomoda un minim 16 lame (blade-uri)

Conectivitate Ethernet	2 x switch-uri 10 Gbps Ethernet cu minim 8 porturi uplink si 16 interne Suport pentru capabilitati de virtualizare Capabilitati de stackare sau tehnologii echivalente a minim 8 switch-uri din cadrul aceleasi familii cu facilitati de vizualizare si propagare a configuratiilor intr-un mod centralizat Capabilitati de partajare a latimii de banda per port Minim 4 x conexiuni 1Gb RJ-45 per sasiu Minim 8 x conexiuni 10Gb per sasiu (fiecare switch instalat in sasiu va trebui sa se conecteze cu platforma de comunicatii pe minim 4 uplink-uri de 10Gbps; in acest sens se vor livra toate componentele necesare realizarii acestor conexiuni)
Conectivitate SAN	2 x switch-uri 8 Gbps FibreChannel cu minim 8 porturi uplink si 16 interne Toate porturile populate cu SFP-uri „short wave”
Integrare ETH/FC	Optional se poate realiza la nivel blade si switch in sasiu unificarea retelei interne ETH/FC prin protocoale tip FCoE.
Management sistem	Procesoare dedicate si redundante on-board - asigura set-up-ul si controlul intregului sasiu; - inventariaza si toate dispozitivele din sasiu ; - ofera informatii legate de temperatura si consum in timp real pentru fiecare server in parte, precum si pentru intregul sasiu; - dispune de un display frontal cu taste pentru a facilita operarea din DataCenter Software de management dedicat care asigura atat managementul serverelor discrete cat si al serverelor virtuale, intr-un mod unitar. Acesta va asigura vizibilitatea starii de buna functionare pentru intreg ansamblul pe o pagina unica, permitand personalului de administrare sainvestigheze diferitele alarme prin accesare detalii in mod ierarhic efectuate prin selectari simple cu mouse-ul, fara a fi necesar sa lucreze in aplicatii multiple. Prin software-ul de management se vor asigura functionalitati de limitare a consumului ansamblului si masurarea puterii consumate pentru fiecare server in parte. Este asigurat controlul de la distanta al oricarui tip de activitate pentru serverele instalate in enclosure: rebootare, instalari OS, preluare ecran la distanta, activitati de depanare. Functionalitatile minime asigurate vor include: - Vizualizare event-uri, monitorizarea starii de buna functionare, colectare date de inventar, descoperire si identificare optiuni hardware instalate, raportare software; - Capabilitati de management de la distanta pentru administrare curenta si pentru asistenta tehnica in caz de incidente; - Capabilitati de console replay pentru review si documentare incidente tehnice sau activitati de administrare; - Capabilitati de a transmite de la distanta comenzi de power-on si power-off; - Posibilitatea de a virtualiza de la distanta unitati de CD-ROM/DVD pentru efectuarea instalarilor de software de catre administrator; - Accelerarea instalarilor de imagini software si sistem de operare; - Simplificarea inventarierii si instalarii patch-urilor corectoare; - Masurarea conditiilor termice de operare.

5.2.2 Server baze de date

Serverele de baze de date se vor instala in sasiul de servere lamelare, vor fi compatibile cu acesta si vor avea urmatoarea configuratie:

CARACTERISTICA	**Specificatie tehnica**
Procesor	Serverul va fi echipat cu minim 2 procesoare de 8 core-uri fiecare in tehnologie CISC x86, la o frecventa de minim 2.6 GHz, avand 20 MB cache L3 Serverul trebuie sa fie upgradabil la 4 procesoare
Memorie	96 GB DDR3 RDIMM Expandabil la 1024 GB Serverul trebuie sa aiba capabilitati de protectie a memoriei de tipul Advanced ECC, Data bus ECC, izolare DIMM, scrubbing, control termal
Controlor HDD	Serverul va fi echipat cu un controller SAS cu interfete 6Gbps si posibilitati de RAID 0,1

Unitati de disk interne	Serverul va fi echipat cu minim 2 diskuri SAS DP 600GB 10.000 rot/min
Controlor retea	Serverul va fi echipat cu 2 interfete 10Gbps Ethernet cu capabilitati de partajare a latimii de banda per port
Controlor fibre channel	Serverul va fi echipat cu 2 interfete 8Gbps FibreChannel
Sloturi I/O	Serverul va fi echipat cu 3 interfete de tip PCIe 3.0 care vor putea acomoda carduri de extindere a interfetelor de comunicatii/conectivitate
Management	Serverul va dispune de procesor dedicat pentru activitati de remote management
Form factor	Server lamelar de tip blade

5.2.3 Server lamelar virtualizare

Serverele de suport pentru solutia de virtualizare se vor instala in sasiul de servere lamelare, vor fi compatibile cu acesta si vor avea urmatoarea configuratie:

CARACTERISTICA	**Specificatie tehnica**
Procesor	Serverul va fi echipat cu minim 2 procesoare de 8 core-uri fiecare in tehnologie CISC x86, la o frecventa de minim 2.6 GHz, avand 20 MB cache L3 Serverul trebuie sa fie upgradabil la 4 procesoare
Memorie	256 GB DDR3 RDIMM Expandabil la 1024 GB Serverul trebuie sa aiba capabilitati de protectie a memoriei de tipul Advanced ECC, Data bus ECC, izolare DIMM, scrubbing, control termal
Controlor HDD	Serverul va fi echipat cu un controller SAS cu interfete 6Gbps si posibilitati de RAID 0,1
Unitati de disk interne	Serverul va fi echipat cu un dispozitiv de tip memorie flash pe care se va instala hipervizorul solutiei de virtualizare
Controlor retea	Serverul va fi echipat cu 2 interfete 10Gbps Ethernet cu capabilitati de partajare a latimii de banda per port
Controlor fibre channel	Serverul va fi echipat cu 2 interfete 8Gbps FibreChannel
Sloturi I/O	Serverul va fi echipat cu 3 interfete de tip PCIe 3.0 care vor putea acomoda carduri de extindere a interfetelor de comunicatii/conectivitate
Management	Serverul va dispune de procesor dedicat pentru activitati de remote management
Form factor	Server lamelar de tip blade

5.2.4 Server rack-abil

Serverele de suport pentru solutia de securitate si autentificare vor avea urmatoarea configuratie:

CARACTERISTICA	**Specificatie tehnica**
Procesor	Serverul va fi echipat cu minim 1 procesoar de 6 core-uri in tehnologie CISC x86, la o frecventa de minim 2.6 GHz, avand 15 MB cache L3 Serverul trebuie sa fie upgradabil la 2 procesoare
Memorie	32 GB DDR3 RDIMM Expandabil la 768 GB Serverul trebuie sa aiba capabilitati de protectie a memoriei de tipul Advanced ECC
Controlor HDD	Serverul va fi echipat cu un controller SAS cu interfete 6Gbps si posibilitati de RAID 0,1
Disk	Doua dskuri de 300GB SAS 6Gbps la 10.000 rot/min
Controlor retea	Serverul va fi echipat cu 4 interfete 1Gbps Ethernet
Sloturi I/O	Serverul va fi echipat cu 3 interfete de tip PCIe 3.0 care vor putea acomoda carduri de extindere a interfetelor de comunicatii/conectivitate
Management	Serverul va dispune de procesor dedicat pentru activitati de remote management
Alimentare	Surse de alimentare redundante, hot plug 220V 50Hz
Form factor	1U rack 19”

5.2.5 Sistem de stocare

Sistemul central de stocare va deserve toate aplicatiile din sistem si va avea urmatoarea configuratie:

CARACTERISTICA	Specificatie tehnica
Arhitectura	Activa-Activa astfel incat un LUN sa fie accesibil prin toate controloarele simultan, cu virtualizare atat pentru spatiul de date cat si pentru spatiul de rezerva.
Tip HDD suportate	SAS, S-ATA (SAS NL), SSD in incinte SFF sau/si LFF Suport pentru minim 450 de discuri distribuite in minim 2 nivele de perfomanta pe discuri SAS(10k/15k) si S-ATA(7.2k) Suport pentru minim 180 de discuri de tip SSD SLC
Capacitate instalata	85.6 TB raw capacitate instalata. Capacitatea va fi compusa din minim 1.6 TB raw din unitati de tip SSD de maxim 100 GB fiecare, minim 80 discuri SAS de 10K RPM de maxim 450GB fiecare, iar diferenta sa fie compusa din discuri SAS de 10K RPM de maxim 1 TB fiecare.
RAID	RAID 0, 1, 5 si 6
Nr Controloare	Minim 4
Cache	60 GB instalat nativ in unitatea de stocare pentru asigurarea unei inalte disponibilitati si performante crescute.
Conectivitate	Fibre Channel, iSCSI
Conectivitate SAN	Minim 8 x 8Gbps FibreChannel instalat
Form factor	Rackabil – compatibil cu Rack echipamente
Asigurarea disponibilitatii	Controloare duale, capabile sa sustina functionalitatile intregului ansamblu in caz de defectare de tip activ-activ astfel incat o singura unitate logica sa poate fi accesata de ambele controllere in acelasi timp. Sistemul ofertat va fi configurat pentru asigurarea unei inalte disponibilitati cu “No Single Point of Failure” pentru controllere, memorie cache, ventilatoare si surse de alimentare Mecanisme de protectie a datelor existente in memoria cache prin scriere pe o memorie de tip non-volatila, in cazul unor caderi de tensiune electrica. Suport de upgrade firmware on-line pentru controllere si discuri. Surse de alimentare redundante, cu baterii integrate pentru protectia cache-ului. Suport nativ fara echipamente suplimentare pentru replicare locala si/sau la distanta prin intermediul protocolului iSCSI. Posibilitatea de upgrade de firmware fara scoaterea sistemului din functiune.
Functionalitatile echipamentului	Aplicatie care asigura provizionarea sistemului de stocare in functie de cerintele aplicatiilor cu posibilitate de definire a unor rutine de provizionare pe diverse grupuri de aplicatii, precum si raportarea statistica in functie de utilizarea discurilor per aplicatie. Capabilitati de tip „thin provisioning” licentiate pentru intreaga capacitate a echipamentului, in cazul unor upgrade-uri ulterioare nefiind necesara achizitionarea unor noi licente. Aplicatie care permite realizarea de clone (point-in-time <PIT> snapshopts), minim 120 de copii de tip PIT. Aplicatie care ofera capabilitati pentru „storage tiering” manual si/sau automat in functie de nevoile aplicatiilor. Datele se vor grupa pe 3 nivele de performanta corespunzatoare celor 3 tipuri de discuri suportate de sistem. Aplicatie care ofera capabilitati pentru transportul automat al datelor intre mai multe echipamente, printr-o modalitate transparenta pentru aplicatii, cu scopul de a mentine o incarcare uniforma pentru intreg ansamblul. Posibiltati de management prin sesiuni de tip telnet, SSH si SMI-S. Aplicatie pentru realizarea de snapshot-uri consistente pentru medii virtuale. Suport pentru realizarea de snapshot-uri consistente pentru urmatoarele aplicatii si baze de date: Microsoft SQL, Microsoft Exchange, Oracle, VMware vSphere, VMware vCenter.

5.2.6 Sistem de backup D2D

In cadrul sistemului se va livra si implementa un sistem de backup de tip disk-to-disk care sa asigure o copie de siguranta a datelor critice din sistem. Platforma livrata deserve toate aplicatiile din sistem si va avea urmatoarea configuratie:

CARACTERISTICA	**Specificatie tehnica**
Capacitate licentiata	24 TB
Numar de clienti	nelimitat
Unitati de disc instalate	SATA, 7200 RPM, de maxim 1TB fiecare
Interfata gazda	8 Gb Fibre Channel (2 porturi) 10 GbE (2 porturi) 1Gb Ethernet (2 porturi)
Rata de transfer	Posibilitate de transfer 10 TB/ ora
Cartuse de banda emulate	Minim 100000
Unitati de banda emulate	Ultrium LTO-2/LTO-3/LTO-4/LTO 5, generic D2D
Suport RAID	RAID6
Alte functii	Deduplicare
Format	Instalabil in rack 19”
Software backup	Solutie de backup cu urmatoarele caracteristici: • Licentiata pentru intreaga capacitate a sistemului de backup (24 TB) care sa aiba inclus agenti de backup pentru sistemul de stocare si gestiune a bazelor de date relational ofertat si serverele de aplicatii. • Protectie automata, pe baza de politici, pentru infrastructurile fizice si virtuale. • Abilitatea de a administra si opera dispozitive de backup atat fizice cat si virtuale. Integrare cu solutia de virtualizare propusa. • Management centralizat al transferurilor de date pentru backup, replicare si stocare pe termen lung intre clienti si dispozitivele de backup, locale sau distante. • Mecanisme de snapshot si restaurare instantanee in conjunctie cu sistemul de backup propus. • Restaurare granulara (de elemente individuale) din cadrul unui backup. • Administrarea centralizata a operatiunilor de backup si restaurare peste sisteme hipervizor, cu suport de snapshots si replicare pentru VMware, Hyper-V si Citrix-Xen. • Integrare cu Active Directory • Agenti cu suport pentru sisteme de operare: Windows /XP/2003/2008/Vista/7/2008 R2; Novell OES; HP-UX; Sun Solaris; Linux Red Hat/SUSE/Debian/OEL/CentOS,; IBM AIX; SGI IRIX; SCO OpenServer; OpenVMS; MacOS • Agenti de backup cu suport pentru: Oracle, Informix, Sybase, MS SQL Server, MS SQL, MS Exchange, MS SharePoint, MS DPM, SAP, SAP DB/MaxDB, Baan IV, Lotus Notes, Lotus Domino, DB2, Autonomy LiveVault

5.2.7 Rack si accesorii

Toate echipamentele vor fi instalate in camera tehnica in rack metallic de 19”, prevazuti cu consola TFT, switch KVM si UPS cu urmatoarele caracteristici:

CARACTERISTICA	**Specificatie tehnica**
Format	42U

Accesorii	Usi perforate pentru optimiarea circulatiei aerului si a disiparii de caldura, kit de stabilizare, panouri laterale
Priza multipla alimentare electrica	4 prize multiple pentru alimentare redundanta, dimensionate conform echipamentelor ce se monteaza in rack-urile respective Rack-ul se va conecta la sistemul de alimentare cu energie electrica furnizat prin intermediul sistemului UPS cu care se va dota DataCenter-ul.
Consola TFT	
Ecran	TFT LCD, 17”, rata improspatare 60-75 Hz, dot pitch 0.26 mm
Rezolutie	1440x900
Pointing device	Touchpad cu 3 butoane si scroll-bar
Conectivitate	PS/2 si USB
Accesorii	Switch KVM IP, 8 porturi, adaptoare USB si cabluri incluse

5.2.8 Statie de lucru

Pentru administrarea componentelor sistemului se va livra o statie de lucru cu urmatoarele caracteristici:

CARACTERISTICA	**Specificatie tehnica**
Procesor	Procesor dual core, 3.4 GHz, 3MB cache L3
Memorie	4GB DDR3-1600
Unitate de disc interna	500 GB, SATA, 7200K RPM
Unitate de disc optic	16X DVDRW, SATA
Adaptor video	Integrat, 1440x900 @ 32bit
Adaptor retea	1Gbps Ethernet
Display	LED LCD, diagonala 18”, 1440x900
Accesorii	Mouse optic, 3 butoane, scroll, USB Tastatura USB

5.2.9 Dispozitive criptografice

Dispozitivele criptografice utilizate pentru pastrarea cheilor Autoritatii de Certificare, semnarea certificatelor emise, a CRL-urilor, procedura de recuperare a cheilor private de criptare, serviciile de validare a starii certificatelor, de marcare temporala si aplicatia de creare a semnaturilor electronice trebuie sa indeplineasca urmatoarele caracteristici:

CARACTERISTICA	**Specificatie tehnica**
Procesor criptografic	Min. 32 biți
Număr de chei stocate	Nelimitat
Certificare	FIPS 140-2 level 3
Interfața de conectare	2xEthernet
Suport standard	PKCS#11
Acces la chei	Suport pentru implementarea de scheme prag pentru acces la chei
Backup	Suport pentru backup-ul si restaurarea materialului criptografic
Criptare simetrică	Suport pentru criptare simetrica: DES, 3DES,AES
Algoritmi de rezumat	Suport pentru algoritmi de rezumat (hash): SHA-1, SHA-2, RIPEMD160
Generare chei asimetrice	RSA, minim 1024 biți on-board
Creare de semnătura	RSA, on-board
Redundanta la nivel hardware cu componente schimbabile în locație	Surse de alimentare Sisteme de ventilație

5.3 Platforma de comunicatii

In cadrul sistemului se va livra si instala o platforma de comunicatie centrala, unificata, omogena si interoperabila care sa asigure toate functiile de comunicatii Ethernet aferente solutiei propuse. Aceasta va avea urmatoarele caracteristici:

CARACTERISTICA	**Specificatie tehnica**
Sasiu/Arhitectura	Rackabil Arhitectura modulara, distribuita L2 si L3, cu minim 5 sloturi: 2 pentru Management/Switch Fabric si minim 3 pentru module de retea, cu o densitate de porturi de pana la 26 porturi de 10Gbps sau 140 porturi de 1Gbps si module de servicii cum ar fi: IPS, SSL VPN, Firewall si IPSec VPN, Load Balancing. Backplane de tip pasiv.
Echipare	2 x Module Management/Switch Fabric ce functioneaza simultan, balansat si redundant si ofera o performanta de pana la 380Gbps fiecare si faciliteaza minim 48Gbps/slot modul retea. Fiecare modul ofera : 1 x RJ45 de tip serial pentru consola, 1 x RJ45 de tip Ethernet 10/100/1000Mbps pentru management out of band 2 x 10Gbps echipate cu 10Gbase-SR, FO MM, 850nm, 300m Modul cu 48 x 1Gbps (capabile PoE), tip Rj45 si urmatoarele performante : - 120 000 adrese MAC - 120 000 rute Ipv4 - 60 000 rute ipv 6 - OAM 802.1ag - MPLS, MPLS VPN L2/VPLS si L3 - Multi-VRF **Modul Firewall/VPN cu urmatoarele facilitati:** - 2 x 1Gbase-T si 2 x 1Gbps combo (1Gbase-T sau SFP) - 1 x Port USB - 1 x Port Serial Consola - 6 Gbps throughput Firewall - 1.8 M sesiuni concurente - 50K Sesiuni pe secunda - 18,000 politici de securitate - 2Gbps 3DES throughput - 8000 tunele L2TP - 5000 tunele IPSec - 4096 tunele GRE - 4000 VLAN-uri - Packet Filtering - ACL extinse/avansate, bazate pe timp, MAC - 250 Firewall-uri Virtuale - 250 zone de securitate - Dynamic Packet Filtering Support firewall pentru : DNS, FTP, ILS, NBT, MSN, PPTP, SIP, HTTP, SMTP, RTSP, H.323, MGCP, Blocare Java/Active X, Pachete fragmentate Urmarirea starii protocoalelor si verificarea conformitatii acestuia cu standardul Protectii la : Land, Smurf, Fraggle, WinNuke, Ping of Death, Tear Drop, IP spoofing, SYN flood, ICMP flood, UDP flood, DNS Query flood si ARP spoofing defense, ARP active reverse lookup, TCP flag packet attack defense, TCP Intercept, Large ICMP packet attack defense, Address/port scanning defense, DoS/DDoS, Filtru protectie SQL Injection Mod de functionare: Firewall Transparent, Routing, Mixt Protectie aplicatii P2P (BT, eDonkey) cu limitare largime de banda NAT ALG pentru: DNS, FTP, MSN, H323, RTSP, SQLNET, SIP, PPTP, ICMP, TFTP, HTTP, Filtrare e-mail: SMTP – adresa e-mail (sursa si destinatie), subiect e-mail, continut e-mail, atasament e-mail (nume si continut), dimensiune mail; POP3 - mail address (sursa si destinatie), Mail subject, Mail attachment (nume si continut) 4k subinterfete vlan

	Filtrare web: URL Hostname, URL IP, HTTP Header, HTTP Body, ActiveX, Java Applet Disponibilitate: Active/Active, Active/Pasive cu sincronizare: configurare politici firewall, sesiuni firewall, SA-uri VPN IPSec **Modul IPS cu urmatoarele facilitati:** 2 x 1Gbase-T si 2 x 1Gbps combo (1Gbase-T sau SFP) 1 x Port Serial Consola Throughput inspectie: 1.2Gbps Sesiuni concurente: 5,000,000 Conexiuni noi pe secunda: 75 000 Detectare atac bazata pe semnatura Detectare atac bazata pe anomalie protocol Inspectia pachetului la nivel de header si payload Detectare de tip multi-tier pentru inspectie paralela a unui flow in hardware Motor de securitate cu inspectie bazata pe flow-uri de date Inspectie trafic IPv4 si IPv6 Protectie la nivel de aplicatie (sisteme de operare, aplicatii) Protectia infrastructurii: a largimii de banda si a echipamentelor de retea: routere, firewall Protectie cu blocare sau limitare a ratei (rate limit) a apicatiilor de tip Instant Messaging, Peer-2-Peer, Streaming Media Facilitati de management trafic cu reguli de permitere, blocare, limitare a ratei traficului (rate limit) Captura selectiva de trafic ce traverseaza IPS-ul Producatorul sa ofere filtre recomandate (minim 4000) pentru protectia retelei astfel incat instalarea si managementul lor sa fie rapide si usoare iar protectia sa fie asigurata din momentul aplicarii filtrelor Protectie la nivel de vulnerabilitate (nu doar exploit) Sa includa protectie pentru urmatoarele atacuri: Worm, Virus,Trojan, P2P, VoIP, Phishing, Suspicious, Reconnaissance, Walk-in-Worm, Backdoor, Spyware, DDoS, Bandwidth Hijacking, Blended Threat, DoS: SYN Floods, Established Connection Floods, Connections Per Second Floods, Vulnerability Protection, Attack Tool Protection, Threshold Filters VLAN Translation Posibilitatea instalarii de noi filtre in mod automat, fara interventia utilizatorului de sistem Facilitati de raportare: pentru traficul care face match pe filtru de protectie, pentru fluxuri de date categorisite pe protocol, dimensiune frame, port, atacuri DDOS Disponibilitate: Activ/Activ si Activ/Pasiv Baza de date de semnaturi (IPS) va fi actualizata cu semnaturi la zi ale producatorului pentru minim 3 ani
Management	CLI WEB (HTTPS) SSH Telnet FTP, TFTP, SFTP pentru transfer fisiere Posibilitatea inspectarii calitatii conexiunilor si a serviciilor cu verificare pachete pierdute, delay, jitter Creearea utilizatorilor de sistem de tip ierarhic pentru access la comenzile sistemului SNMP v1, v2c, v3 RMON NTP LLDP Ofera posibilitatea stocarii a doua fisiere de firmware pentru backup in timpul upgrade-ului Syslog Debug

Multicast	IGMP v1/v2/v3 cu utilizare Any-Source Multicast (ASM) si Source-Specific Multicast (SSM) IGMP Snooping MSDP LLDP-MED PIM-DM, PIM-SM, PIM-SSM MBGP Multicast VLAN pentru IPv4 si IPv6 Voice VLAN prin asignare automata a VLAN-urilor si prioritatii pentru telefoane IP
Layer 2	4096 VLAN-uri VLAN bazat pe port, protocol, Subnet IP, MAC Manipulare VLAN (VLAN Mapping): 1:1 (dintr-un VLAN intr-un alt VLAN), N:1 (din mai multe VLAN-uri intr-un alt vlan), 2:2 (QinQ, din 2 vlan-uri (tag interior si exterior) in alte 2 vlan-uri (tag interior si exterior) Private VLAN Guest VLAN pentru 802.1x Tunelare BPDU GVRP Port Mirroring: 4 Grupuri de mirror cu numar nelimitat de porturi / grup de mirror, mirror intre module MLD Snooping RFC 3069 IEEE 802.1ad QinQ Frame-uri Jumbo IEEE 802.1ag Storm Protection: broadcast, multicast, unicast necunoscut
Layer 3	uRPF Graceful Restart for OSPF, BGP, IS-IS UDP Helper VRF Stiva duala IPv4 si IPv6 Tunelare IPv6 DHCPv6 RIP v1/v2, RIPng OSPFv2/OSPFv3 BGP4, MBGP, BGP pentru adresare IPv6 IS-IS, IS-ISv6 ECMP Policy Routing ICMPv6 Tunelare IPv6: IPv6 peste IPv4, ISATAP MPLS, MPLS L3 VPN, MPLS L2 VPN, VPLS
QoS	Clase de trafic bazate pe ACL standard si extinse pe baza adresa MAC, adrese IP sursa si destinatie (IPv4 si IPv6), protocol, port Remarcarea pachetelor cu 802.1p, Precedenta IP, si DSCP 8 cozi de prioritizare per port Precedenta 802.1p Precedenta DSCP,ToS Scheduling: SP, WRR, SP+WRR, WFQ Evitarea congestiei: WRED, Tail-Drop Traffic Shapping Traffic Metering Traffic Accounting Traffic Policing: Commited Access Rate (intrare , iesire): granularitate 64kbps
Securitate	ACL IPv4 si IPv6 ACL standard si extinse ACL bazate pe VLAN ACL de tip ingress/egress 802.1X cu posibilitate asignare dinamica a facilitatilor de QoS, ACL si VLAN

	precum si integrarea intr-o solutie de Network Access Control (NAC) uRPF 802.1X Server IP Source Guard ACL bazate pe perioada de timp Sa suporte module de IPS, Firewall si VPN/IPSec, VPN SSL
Disponibilitate si fiabilitate	Sa suporte topologie de tip inel cu o convergenta de sub 100ms Pentru o inalta disponibilitate si o omogenitate a solutiei, platforma de comunicatii trebuie sa suporte tehnologii de virtualizare astfel incat solutia propusa sa fie interconectata la nivelul echipamentelor prin interfete Ethernet de 10Gbps (min 4 interfete de interconectare per switch), si sa ofere: - O singura adresa IP si un singur fisier de configurare pentru toate echipamentele interconectate - Link Aggregation Distribuit pentru conectarea altor echipamente de retea: switch-uri, servere - Distributed Routing si distributed switching - Echipamentele interconectate trebuie sa se comporte ca un singur Nod Layer 2 si Layer 3 (o singura adresa IP din perspectiva protocoalelor de rutare, MPLS) - Suport pentru topologie Ring sau Daisy-Chain - Posibilitatea ca echipamentele interconectate sa fie distribuite geografic (la distante mai mari de 100m) Redundanta 1+1 la nivel de switch fabric (cu load sharing) Redundanta 1+1 la nivel de sursa de alimentare Backplane pasiv Toate modulele sunt de tip HotSwap BFD VRRP Cai diferite pentru Control si Servicii astfel incat un anumit serviciu configurat sa nu influenteze controlul asupra echipamentului.
Monitorizare si troubleshooting	Port Mirroring, Remote Port Mirroring, Mirroring intre module Flow Mirroring OAM – IEEE 802.3ah IEEE 802.1ag
Memorie	64 MB flash, 512 MB SDRAM
Throughput	270 millions pps
Marime tabela de routare	250000 intrari ipv4, ipv6
Marime tabela adrese MAC	500000 intrari
Surse de alimentare Ventilatoare Racire	2 surse de alimentare AC incluse, 220V 50Hz, maxim 1400W, redundanta 1+1 O baterie de ventilatoare Racire fata-spate

5.4 Amenajare DataCenter

Trebuie sa asigure, tinand seama de caracteristicile proprii sistemelor operate (inalta dependenta de TI, costuri inalte penru intrerupere, inalta scrutinitate), maximum 22 h/an de indisponibilitate (99,75%).
In cadrul lucrarilor de amenajare a acestui DataCenter se vor realiza activitati de recompartimentare a spatiului disponibil in vederea separarii zonei de echipamente, de zona desemnata operatorilor umani.
Solutia propusa pentru DataCenter va avea in vedere evitarea urmatoarelor situatii:

- intreruperea furnizarii serviciilor;
- efractia si accesul neautorizat;

Pentru asigurarea unei disponibilitati ridicate a sistemului se vor prevedea urmatoarele:

- asigurarea alimentarii rack-urilor de echipamente cu energie electrica pe doua ramuri in vederea evitarii intreruperilor in functionare,
- se va achizitiona un UPS cu o capacitate de minim 50kVA, autonomie de minim 4 minute la incarcare maxima, care va asigura functionarea tuturor echipamentelor,

- pentru alimentarea cu energie electrica a echipamentelor nou instalate se va realiza o instalatie separata de cea a cladirii. Aceasta instalatie va contine tablouri de distributie, circuite si elemente de conectare.
- instalarea unui sistem de climatizare pentru evitarea defectelor datorate supraincalzirii. Capacitatea acestui sistem va fi de minim 50kW.
- sistemul de climatizare va fi prevazut cu protectii suplimentare pentru asigurarea functionarii sistemului de conditionare a aerului 7 zile/7 zile, 24h/24h

Lucrari:
necesar spatiu amenajat: aproximativ 95 mp din care 70 mp spatiu camera tehnica, 25 mp birouri

dotarea spatiului existent cu pardoseala flotanta acoperita cu izolare PVC antistatica

structura de sustinere a panourilor de pardoseala ranforsata pentru distribuirea greutatii astfel incat sa nu se depasesca sarcina maxima per MP comunicata de constructorul cladirii

se va instala un plafon fals, casetat

anularea tuturor tevilor de alimentare cu agent termic catre radiator. Izolarea (pana la coloanele principale).

in vederea securizarii locatiei, necesitatea anularii/izolarii geamurilor catre exterior.

utilizarea de material izolant cu poliestiren expandat si placi de gips carton rezistente la foc pentru geamurile exterioare.

dotarea locatiei cu sistem de stingere a incendiului pe baza de gaz inert, conform standardelor in vigoare.

dotarea locatiei cu sistem de control al accesului (tehnologie RFID) atat in zona destinata operatorilor umani, cat si in zona de echipamente avand scopul de a restrictiona, selecta si ordona miscarea persoanelor in interiorul zonelor definite, prin verificarea dreptului de acces a fiecarei persoane care solicita accesul in zona.

Cablare:
infrastructura pentru reteaua LAN va fi realizata prin cablare structurata FTP cat.6.

toate cablurile (atat cele de date, cat si cele de alimentare) vor fi dispuse in canale de cabluri metalice, separate, prevazute cu capac si conectate la centura de impamantare. Aceste canale de cabluri vor fi dispuse sub podeaua tehnologica si deasupra plafonului fals.

toate zonele in care vor fi dispuse cabluri vor fi prevazute cu senzori de fum si temperatura conectati la sistemul de securitate al centrului.

pentru toate conexiunile de date se vor prezenta rapoarte de testare, certificare cat.6.

Pentru realizarea unui acces controlat al adminsitratorilor de sistem si al personalului tehnic in spatiul dedicat DataCenter se va prevedea realizarea unui sistem de acces in care acestia sa se autentifice cu cardurile de tip SmartCard folosite la autentificarea pe statiile de lucru de administrare si monitorizare. In acest sens, administratorii de sistem vor avea un singur card de tip SmartCard personalizat cu care se vor autentifica pe statiile de lucru pentru administrare si monitorizare si vor realiza accesul in spatiul DataCenter. Se vor prevede un minim de 10 carduri pentru acces in locatiile protejate cu sisteme de control acces.

6. SOFTWARE DE BAZA

6.1 Sisteme de operare

Sistemele de operare care rulează pe servere trebuie să asigure un suport complet al infrastructurii hardware și să furnizeze un înalt nivel de scalabilitate și fiabilitate.
Sistemele de operare trebuie să:

- permită rularea pe procesoare cu 64 biți;
- să permită folosirea unor cantități mari de memorie de cel puțin 64 GB;

- să permită folosirea pe minim 2 procesoare fiecare cu minim 8 nuclee de procesare;
- să ofere instrumente care pot fi rulate din linia de comandă pentru administrarea sistemului;
- să ofere instrumente de diagnosticare, care vă oferă vizibilitate asupra mediului serverului, pentru a identifica și rezolva rapid problemele care apar;
- să aibă suport pentru Internet Protocol versiunea 6 (IPv6);
- suport pentru SAN (Storage Area Network);
- să permită configurarea de cluster fail-over sau să permită rularea de cluster load balancing în funcție de necesități;
- conectare automata și obținerea adresei automate la conectarea în rețea;

Sistemele de operare ofertate trebuie să fie compatibile cu produsele software și aplicațiile furnizate pentru fiecare mașină conform arhitecturii.

6.2 Server de aplicatie

Serverul de aplicații va permite rularea tuturor aplicațiilor dezvoltate în cadrul proiectului. Platforma va îndeplini minim următoarele cerințe:

- Server-ul de aplicație va fi o platformă robustă ce oferă suport pentru rularea de aplicații .NET, J2EE sau echivalent;
- Server-ul de aplicație va oferi facilități de dezvoltare a aplicațiilor, performanță ridicată și administrare simplă;
- Server-ul de aplicație va oferi suport pentru tehnologiile standardizate/larg răspândite și medii de dezvoltare care să permită programarea aplicațiilor în mod facil;
- Server-ul de aplicație va oferi suport pentru WEB 2.0;
- Server-ul de aplicație va oferi suport pentru servicii web;
- Server-ul de aplicație va oferi suport pentru SOAP;
- Server-ul de aplicație va permite structuri de cluster;
- Server-ul de aplicatie va oferi o componentă server web;
- Server-ul de aplicatie va avea facilitati de load balancing si routare integrate la nivel de aplicatie;
- Server-ul de aplicatie trebuie sa permita caching dinamic;
- Server-ul de aplicatie trebuie sa poata accepta sesiuni de tip SSL.

In arhitectura propusa nivelului de aplicatii de date i se vor aloca un minim de 40 core-uri fizice de procesare dedicate.

6.3 Sistem de Stocare a datelor si Gestiune a Bazelor de Date

Pentru stocarea datelor colectate, se va proiecta un model de date flexibil, de tip relational, compatibil cu standardul ANSI SQL.
Modelul de date trebuie sa fie integrat, orientat pe subiect si independent de aplicatie:
Integrat - informatiile despre o aceeasi entitate sunt stocate intr-o singura entitate (tabela) avand un model comun, indiferent daca provine din mai multe surse;

Orientat pe subiect - modelul de date este structurat tinand cont de arii functionale si nu de procese, departamente etc.;

Independent de aplicatie - modelul de date nu trebuie sa depinda de o anumita sursa de date sau de modelul acesteia;

In construirea modelului de date se va face trecerea de la modelul logic la cel fizic astfel:
Modelul logic - este folosit pentru a modela concepte si relatii (entitati, subentitati, atribute, relatii);

Modelul fizic - reprezentarea fizica a modelului logic (tabele, coloane, chei primare, unice si externe, indecsi);

Implementarea tabelelor - reprezinta modul de implementare a modelului fizic la nivelul bazei de date (baza de date, partitii, optiuni de stocare, indecsi). Solutia trebuie sa ofere posibilitatea de partitionare a tabelelor in scopul reducerii timpului de acces la date dupa diverse criterii de partitionare (list, range, hash) si combinatii ale acestora (range-list, range-hash, etc.). De asemenea solutia trebuie sa permita accesul cat mai rapid la informatii si prin utilizarea diferitelor tipuri de indecsi, cum ar fi B-Tree, bitmap, partitioned, function based,

domain sau similari.

Tabele in baza de date - tabelele exista in baza de date si sunt populate cu date;

In arhitectura propusa nivelului de baze de date i se vor aloca un minim de 12 core-uri fizice de procesare dedicate.
Nivelul baza de date include urmatoarele categorii de cerinte detaliate mai jos:

Cerinte generale

SGBDR va fi capabil sa stocheze, interogheze si sa returneze date alfanumerice

Baza de date relationala trebuie sa suporte comunicarea cu aplicatiile client folosind protocolul de transport pe retea TCP/IP

Baza de date relationala trebuie sa ruleze pe pe distributiile majore de sisteme de operare prezente pe piata cum ar fi Windows, Linux, Solaris, AIX, HP-UX, in vederea asigurarii portabilitatatii.

SGBDR va oferi functii de raportare si se va integra usor cu instrumentele de raportare folosite.

SGBDR va suporta Unicode UTF-8 pentru a asigura un set acoperitor de caractere.

Cerinte de securitate

Baza de date relationala va trebui sa permita restrictionarea accesului la nivelul obiectelor bazei de date in functie de drepturile de acces ale utilizatorilor

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 asigure facilitati privind autentificarea, verificarea si restrictionarea drepturilor si permisiunilor de acces la informatii la nivel de camp si inregistrare, in functie de utilizatorul conectat, astfel incat fiecare institutie (SISF, SIS, INS) sa aiba acces doar la subsetul de date care ii este adresat

In vedera auditarii activitatii, baza de date relationala trebuie sa ofere o facilitate care inregistreaza urmatoarele informatii pentru modificari, inserari, stergeri si selectari de catre utilizatori individuali, ale obiectelor interne bazei de date:

id-ul utilizatorului bazei de date (ID asa cum este el stocat in baza de date)

data si ora (data si ora actiunii)

tipul tranzactiei (selectare, inserare, modificare, sau stergere)

id-ul bazei de date

obiectul/obiectele tinta

interogarea trimisa

Baza de date relationala trebuie sa ofere abilitatea de a se ajusta la gradul de detalii, capturate de catre facilitatea de audit.

Baza de date trebuie sa ofere un mecanism de verificare si validare a parolelor.

Baza de date relationala trebuie sa ofere un mecanism de criptare a datelor.

Implementarea conceptului de Multi Level Security si a principiului Need to Know prin etichetarea/clasificarea in mod diferit a randurilor dintr-o tabela in functie de nivelul de acces pe care trebuie sa-l indeplineasca un utilizator pentru a putea accesa acea informatie;

In mod transparent fata de aplicatii, etichetarea si clasificarea datelor la nivel de inregistrare, permitand in acelasi timp si aplicarea mai multe politici de clasificare asupra aceleiasi tabele;

Mecanisme native de restrictionare a accesului utilizatorilor la nivel de inregistrare si coloana intr-o tabela;

Criptarea datelor care sunt stocate in baza de date, la nivel de coloana, tabela sau tablespace, criptare care trebuie sa fie facuta transparent fata de aplicatii fara a fi nevoie de modificari sau dezvoltari suplimentare la nivelul acestora;

Criptarea traficului prin retea intre aplicatia de business sau utilizator si baza de date, pentru a elimina posibilele incercari de interceptare a datelor cand sunt transmise in mediile de comunicatie.

Generarea unei liste cu operatiile pe care un grup sau o clasa de utilizatori le poate executa;

Cerinte de salvare si recuperare

Baza de date relationala trebuie sa ofere o facilitate pentru salvarea totala si/sau partiala a bazei de date

Baza de date relationala trebuie sa ofere o facilitate pentru restaurarea totala si/sau partiala a bazei de date.

Baza de date relationala trebuie sa ofere o facilitate pentru inregistrarea tuturor modificarilor bazei de date, pentru a permite recuperarea bazei de date (inregistrarea tranzactiilor)

Baza de date relationala trebuie sa ofere o facilitate pentru recuperarea totala si/sau partiala a bazei de date de la un moment de timp specificat de utilizator.

Baza de date relationala trebuie sa ofere abilitatea de a face salvari pentru unul sau mai multe spatii alocate tabelelor asa cum este specificat de catre administratorul bazei de date.

Baza de date relationala trebuie sa permita salvarea online a bazei de date direct pe banda.

Baza de date relationala trebuie sa permita o restaurare a bazei de date direct de pe banda.

Baza de date relationala trebuie sa scrie in mai multe fisiere pe disc simultan in timpul unei operatii de salvare, in vederea cresterii performantei.

Baza de date relationala trebuie sa citeasca din mai multe fisiere pe disc simultan in timpul unei operatii de restaurare, in vederea cresterii performantei.

Baza de date relationala trebuie sa permita citirea si scrierea paralela in timpul unei operatii de salvare

Baza de date relationala trebuie sa permita citirea si scrierea paralela in timpul unei operatii de restaurare

Baza de date relationala trebuie sa permita o arhitectura de inalta disponibilitate

Cerinte de integritate a datelor

Baza de date relationala trebuie sa identifice si sa rezolve situatiile care ajung in puncte moarte (deadlock)

Baza de date relationala trebuie sa permita constrangeri de tip cheie primara

Baza de date relationala trebuie sa permita ca o coloana sa nu accepte valori NULL.

Baza de date relationala trebuie sa ofere abilitatea de impunere a constrangerilor pentru a se asigura ca nici o valoare duplicata nu este introdusa intr-o coloana anume care nu participa la o cheie primara

Baza de date relationala trebuie sa ofere abilitatea de a impune constrangeri asupra tipurilor si valorilor datelor

Cerinte privind dictionarul datelor

Baza de date relationala trebuie sa ofere o facilitate de catalog (sau dictionar de date) care este modificata

automat de fiecare data cand instructiuni de tipul Data Definition Language (DDL – Limbajul de definire a datelor) si Database Control Language (DCL - Limbajul de Control al Bazei de Date) se aplica pe acea baza de date.

Baza de date relationala trebuie sa ofere o facilitate pe platforma instalata pentru a accesa catalogul si a obtine informatii legate de obiectele bazei de date, in vedera monitorizarii instructiunilor care se executa.

Cerinte privind performanta si scalabilitatea bazei de date

Baza de date relationala trebuie sa poata rula pe sisteme de tip cluster in mod activ-activ

Baza de date trebuie sa asigure partajarea automata a incarcarii intre nodurile cluster-ului in vederea maririi productivitatii

Sistemul de gestiune de baze de date sa contina propriul soft de clusterware integrat, astfel incat sa permita rularea pe diferite platforme si sisteme de operare fara achizitionarea de soft de cluster aditional de la producatorul sistemului de operare

Baza de date relationala trebuie sa ofere abilitatea sa partitioneze tabele in vederea cresterii performantei si administrarii facile a datelor din tabele

Baza de date relationala trebuie sa permita unei tabele sa fie partitionate bazandu-se pe una sau mai multe valori specifice de date, asa cum este hotarat de catre administratorul bazei de date

Sa ofere posibilitatea de partitionare logica a tabelelor mari in scopul reducerii timpului de acces la date dupa diverse criterii de partitionare (list, range, hash) si toate combinatiile acestora (range-list, range-hash, etc.)

Baza de date relationala trebuie sa permita definirea cantitatii minime de date transferate intre disc si memoria locala a bazei de date la o cerere

Baza de date relationala trebuie sa ofere facilitatea sa retina date din tabele special indicate in memoria locala pentru o perioada nedefinita de timp

Baza de date relationala trebuie sa permita setarea marimii unei zone din memoria locala, rezervata sa retina date din tabele special indicate, pentru o perioada nedefinita de timp

Baza de date relationala trebuie sa aiba un optimizator bazat pe cost pentru a optimiza interogarile

Instante multiple, izolate, si complet functionale ale bazei de date trebuie sa poata coexista pe un singur nod fizic.

Baza de date relationala trebuie sa suporte indecsi in vederea regasirii rapide a informatiilor.

Cerinte privind administrarea bazei de date

Baza de date relationala trebuie sa ofere o unealta de administrare a bazei de date

Unealta de administrare a bazei de date oferita cu Baza de date trebuie sa includa urmatoarele caracteristici:

O fereastra SQL pentru a construi si executa scripturi

O fereastra pentru a salva si afisa scripturi SQL

O fereastra grafica pentru a adauga si sterge urmatoarele obiecte ale bazei de date si pentru a le modifica

proprietatile: tabel, index, vedere, constrangere, declansator, procedura stocata

O interfata pentru a efectua sarcini legate de urmatoarele functii ale bazei de date: stocare, backup, recuperare

Sa ofere capabilitatea de diagnosticare a problemelor aparute la nivelul bazei de date prin urmarirea executiilor

Sa permita prin componenta de administrare web afisarea de grafice de performanta in timp real

Sa ofere o functionalitate de recomandari de optimizare a interogarilor SQL

Solutia pentru baze de date trebuie sa contina multiplii algoritmi de compresie ai datelor bazei de date, cu posibilitatea de estimare a ratei de compresie inainte ca aceasta sa fie aplicata;

solutia pentru baze de date trebuie sa contina mecanisme care permit administrarea volumelor de date,

compresia datelor, salvarea si restaurarea datelor, redundanta datelor;

componentele redundante care asigura stocarea datelor sa ofere catre bazele de date o singura imagine unitara

pentru distribuirea datelor.

6.4 Analiza si raportare (Business Inteligence)

Valorificarea informatiilor de care dispun organizatiile in vederea fundamentarii proceselor decizionale este un proces complex, care de regula angajeaza resurse hardware, software si umane deosebite.
Componenta de analiza si raportare dispune de componente dedicate pentru analiza datelor, adresate rolurilor specifice din cadrul unei organizatii.
Solutia este centrata pe facilitarea utilizatorilor la informatii, interactiunea dintre acestia si datele accesate avand loc intr-un mediu web, intuitiv, in care majoritatea operatiilor pot fi efectuate prin actiuni de tip ‚click' si ‚drag and drop'.
Utilizatorii non-tehnici, dar si cei tehnici au posibilitatea sa interactioneze cu datele intr-o maniera prietenoasa, accesul lor fiind facilitat de un dictionar ce ‚traduce' structurile de date in concepte cu care acestia sunt familiarizati (exemplu: clienti, furnizori, produse, etc).
Usurinta in exploatare pentru utilizatorul final (care isi poate construi propriile rapoarte/grafice, etc, fara sa aiba cunostinte tehnice sau sa cunoasca sursele de date pe care le acceseaza) fac ca aceasta componenta sa reprezinte un instrument ideal in activitatea de analiza si de raportare curenta. Mai mult decat atat, prin accesarea unor surse eterogene de date (baze de date pe platforme diferite, baze de date relationale sau OLAP, sisteme tranzactionale/ de tip datawarehouse), utilizarea unui astfel de instrument asigura o viziune globala, completa, asupra datelor existente in cadrul companiei.
Prin modul in care este conceputa, solutia de analiza si raportare va implementa urmatoarele principii, care sa asigure maxim de beneficiu in procesele de raportare si analiza curente ale organizatiei:
Viziune unica asupra informatiilor institutiei;

Viziune unica din punct de vedere semantic asupra informatiilor;

Accesul facil pentru utilizatori la datele la care au acces;

Acces la date in timp real;

Infrastructura unitara.

Componenta de analiza si raportare va fi folosita de un numar de 20 de angajati si trebuie sa indeplineasca urmatoarele cerinte:
Sa ofere posibilitatea de rulare pe diverse platforme hardware si pe sistemele de operare majore de pe piata (Windows, Linux si UNIX);

Sa ofere posibilitatea prezentarii datelor in formate variate (tabele, tabele pivot, grafice, texte derulante, etc.);

Sa ofere functionalitati de navigare ghidata pentru utilizatorii finali, cu posibilitati multiple de navigare dintr-un anumit punct, atat pentru rapoarte cat si pentru grafice;

Sa permita combinarea rezultatelor obtinute de pe platforme diferite la momentul interogarii, astfel incat setul de date rezultat sa fie unitar;

Sa permita salvarea rapoartelor in formate diferite (Excel, PDF, Word, HTML, etc);

Sa ofere posibilitatea includerii rapoartelor/graficelor in tablouri de bord pentru toti utilizatorii finali, fara costuri de licentiere suplimentare;

Sa permita tuturor utilizatorilor finali modificarea tablourilor de bord sau a rapoartelor (fara costuri de licentiere suplimentare);

Sa nu necesite replicarea datelor pe un server separat, ci sa foloseasca capabilitatile bazei de date sursa. Mediul de lucru pentru utilizatorii finali sau alti dezvoltatori de rapoarte/analize sa fie in mediu web pur;

Sa faciliteze accesul la informatie printr-un nivel de metadate care sa ascunda utilizatorilor finali complexitatea structurilor fizice de date;

Nivelul de metadate expus utilizatorilor sa fie comun la nivelul tuturor modulelor sistemului de raportare si analiza;

Utilizatorii sa isi poata crea singuri propriile rapoarte (analize ad-hoc) fara sa fie nevoiti sa cunoasca structurile fizice de date pe care le acceseaza;

Sa permita accesarea datelor atat de pe platforme relationale, cat si multidimensionale sau foi de calcul;

Sa permita integrarea cu LDAP, oferind in acelasi timp capabilati proprii de definire a rolurilor pentru restrictionarea accesului la rapoarte;

Interactiunea utilizatorilor finali cu aplicatia se va face intr-o interfata de tip web, fara a necesita instalarea de componente software suplimentare pe masinile utilizatorilor, prin operatiuni de tip point-and-click si drag-and-drop;

Sa expuna o interfata de administrare atat a drepturilor de acces la diferite zone cat si a drepturilor de acces pe diferite tipuri de actiuni;

Sa fie scalabila si sa dispuna de mecanisme de clustering a componentelor (de prezentare sau la nivel de server de acces la date), astfel incat sa poata fi adaugate ulterior resurse hardware suplimentare;

Sa ofere posibilitatea prezentarii simultane a aceleiasi informatii in formate diferite, printr-o singura executie a interogarii: de exemplu tabel + grafic;

Sa permita configurarea raportului astfel incat utilizatorii sa poata selecta in tabloul de bord modul de reprezentare a informatiei: tabel, grafic, etc;

Sa permita facilitati avansate de formatare a rapoartelor;

Sa ofere posibilitatea de salva, organiza si partaja rapoartele cu alti utilizatori;

Sa ofere capabilitati de drill-down pe diferite nivele de agregate;

Generarea interogarilor catre bazele de date sa tina seama de specificul bazei de date accesate – sa genereze interogarile tinand cont de functii native, specifice ale fiecarei platforme in parte;

Sa ruleze pe o instanta de baza de date separata fata de cea de productie dar identica ca si continut cu aceasta; baza de date pentru operatiile solutiei de analiza si raportare va rula intro masina separata de cea de productie cu resurse de memorie si procesare dedicate; pentru baza de date care va deservi rularea operatiilor de analiza si raportare se vor aloca un minim de 2 core-uri fizice ca resursa de procesare dedicata.

Produsul va oferi posibilitatea de a crea rapoarte inlantuite, datele din raportul copil fiind filtrate pe baza rezultatelor din raportul parinte;

Accesul utilizatorilor la informatie trebuie sa se faca si pe criteriul domeniului de valori (de exemplu un utilizator

sa nu poata vedea decat randurile la care acces);

Sa ofere acces direct la surse de date multiple, de pe platforme diferite, incluzand surse Oracle si non-Oracle (SQL Server, DB2, SQL Anywhere, etc.), in mod transparent pentru utilizatorul final;

Sa dispuna de mecanisme de alertare pentru utilizatorii finali (cel putin prin aplicatie, email si dispozitive mobile);

Accesul utilizatorului final sa se faca dintr-o singura interfata web din care sa aiba acces la toate componentele de analiza, raportare, alertare, notificare, etc.

Sa ofere utilizatorilor finali posibilitatea subscrierii la alertele definite;

Sa dispuna de mecanisme de optimizare a accesului la informatie (cu impact minim asupra bazei de date) asigurand minimal urmatoarele: mecanisme de multi-user shared caching, generarea optimizata a interogarilor;

Din punctul de vedere al arhitecturii sistemului de raportare, toate componentele sale trebuie sa fie strans integrate, sa faca parte dintr-un mediu unitar de lucru si sa impartaseasca un sistem de securitate comun;

Produsul trebuie sa afiseze exceptiile/depasirile sub forma de cod culori;

Sa ofere utilizatorilor posibilitatea agregarilor personalizate pe nivel, atat in baza de date, cat si in aplicatia de front-end.

Sa asigure acces ODBC catre layer-ul de metadate ce poate fi accesat direct de catre orice alta aplicatie

Sa asigure posibilitatea de writeback in baza de date din layer-ul de raportare.

Sa ofere posibilitatea de a copia obiectele din tablourile de bord si de a le afisa in MS Office

Sa ofere utilizatorului posibilitatea de a utiliza acelasi set de parametrii catre multiple rapoarte/ tablouri de bord.

Sa ofere utilizatorilor posibilitatea agregarilor personalizate pe nivel, atat in baza de date , cat si in aplicatia de front-end

Sa ofere capabilitati pentru salvarea filtrelor aplicate unui raport sau pentru salvarea template-urilor de formule

Sa dispuna de vizualizari interactive, tranzitii animate intre rapoarte, legaturi Master – Detail

6.5 Platforma virtualizare

Produsul software de virtualizare se va instala pe serverele de lamelare de virtualizare, va fi licentiata corepunzator pentru intreaga capabilitate a masinilor si va trebui sa indeplineasca minimal urmatoarele cerinte:
Cerinte generale:

- Sa nu depinda de un sistem de operare gazda a carui actualizare sa afecteze disponibilitatea si functionalitatea serverelor, respectiv a masinilor virtuale care ruleaza pe serverele respective.
- Amprenta pe disc mica a hypervisor-ului; instalarea hypervisor-ului sa poata fi facuta rapid (direct pe servere), chiar si din retea, atat pe discuri locale (HDD) cat si pe unitati de stocare flash USB si SSD.
- Sa ofere posibilitatea crearii unor profile pentru host-uri (servere fizice) astfel incat instalarea pe mai multe host-uri sa se faca foarte rapid, respectand o configuratie prestabilita, eliminand erorile de configurare si oferind totodata posibilitatea modificarii parametrilor configuratiei.

Caracteristici de virtualizare:

- Distributie automata a masinilor virtuale pe nodurile platformei de virtualizare, pe baza de reguli de afinitate si anti-afinitate.
- Sa poata rula pe servere ce contin pana la 128 de core-uri logice si 2 TB memorie RAM.
- Sisteme de operare suportate pe masinile virtuale: Microsoft Windows, Red Hat Enterprise Linux, SuSE Linux Enterprise Server, Netware, Solaris, Oracle Enterprise Linux.
- Aplicatia de virtualizare trebuie sa poata permite crearea de masini virtuale cu pana la 64 procesoare virtuale si 1 TB RAM.
- Aplicatia si sistemul de fisiere asociat trebuie sa poata permita adaugarea de procesoare virtuale, memorie RAM, interfete de retea si hard disk-uri la masinile virtuale fara a necesita oprirea acestora.
- Aplicatia de virtualizare trebuie sa permita crearea de grupuri de masini virtuale care sa imparta aceleasi resurse puse la dispozitie in comun (memorie si timpi de procesor).
- Software-ul instalat pe host trebuie sa poata crea echipamente de retea virtuale (switch-uri) la care sa se conecteze masinile virtuale si interfetele de retea fizice de pe host.
- Suport pentru dispozitive USB conectate direct in host (nod de virtualizare); dispozitivele USB vor putea fi accesate de catre sistemele de operare instalate in masina virtuala.
- Protectia masinilor virtuale impotriva programelor de tip virus sau malware, fara a fi necesara rularea de agenti dedicati in masinile virtuale in cauza.

Inalta disponibilitate:

- Configurarea in clustere de inalta disponibilitate cu pana la 32 de host-uri.
- Sa dispuna de capacitati de failover astfel incat, in cazul defectarii unui host, masinile virtuale care rulau pe acel host sa fie restartate pe alte host-uri din cluster.
- Sa ofere posibilitatea mutarii simultane a masinilor virtuale in functiune (minim 4, pe legaturi Gigabit/10Gigabit) de pe un host pe altul/altele fara afectarea functionarii acestora, pentru a se putea executa activitati de mentenanta pe host-ul respectiv.
- Sa ofere balansarea automata a incarcarii pe host-urile din cluster prin mutarea masinilor virtuale in vederea asigurarii resurselor optime pentru functionare.
- Sa ofere mecanisme automate de economisire a energiei electrice prin concentrarea masiva a masinilor virtuale pe cateva host-uri si oprirea host-urilor nefolosite in momentul in care incarcarea masinilor virtuale scade. In mod similar, atunci cand incarcarea masinilor virtuale creste, host-urile nefunctionale vor fi pornite in vederea asigurarii resurselor computationale corespunzatoare prin balansarea automata a incarcarii pe fiecare host din cluster.

Memorie:

- Partajarea transparenta a paginilor de memorie, pentru toate sistemele de operare (in masina virtuala) suportate. Paginile de memorie virtuala cu continut identic vor fi stocate intr-o singura instanta (o singura data) la nivelul memoriei fizice.
- Mecanisme de compresie a memoriei, pentru toate sistemele de operare (in masina virtuala) suportate.

- Mecanism de alocare a memoriei fizice catre masinile virtuale pe baza de actiuni (shares), cu posibilitatea de garantare si limitare superioara a memoriei alocate.

Stocare:

- Sa suporte diverse tipuri de storage (SAN, NAS) si protocoale de access (FC, FCOE, iSCSI, NFS).
- Sa permita prioritizarea accesului la storage pentru masinile virtuale, la nivel de cluster.
- Posibilitatea utilizarii unui echipament de stocare extern pentru mai multe host-uri; storage-ul trebuie sa poata stoca atat masina virtuala cat si hard disk-urile virtuale asociate acesteia.
- Accesul catre sistemul de stocare extern sa poata fi facut pe mai multe cai (multipathing), asigurandu-se suport pentru fail-over si load balancing si avand posibilitatea de alegere a politicii de stabilire a caii (fixa, MRU, Round Robin).
- Sistemul de fisiere va permite accesul concurent al mai multor servere fizice (host) si al mai multor masini virtuale la aceasi resursa de stocare.
- Sistemul de fisiere trebuie sa asigure ca o masina virtuala este accesata doar de pe un singur host (sistem de blocarea accesului); in caz de defectare a host-ului masina virtuala trebuie sa poata fi restartata de pe alt server fizic.
- Sistemul de fisiere va asigura posibilitatea migrarii in timp real (fara intreruperea functionarii) unei masini virtuale de pe un host pe altul, de pe o capacitate de stocare pe alta.
- Sa ofere posibilitatea executarii operatiunilor de mentenanta sau upgrade la storage fara afectarea functionarii masinilor virtuale.
- Controlul activitatilor de I/O pentru accesul la storage.
- Mecanism de distributie automata a volumelor de discuri virtuale pe diferite echipamente de stocare in functie de necesarul de performanta in accesarea acelor discuri precum si de performanta oferita de echipamentele de stocare disponibile.
- Managementul resurselor de stocare (QoS)
- Distributie automata a sarcinii (load balancing) pe adaptoarele de acces la storage.
- Sistemul de fisiere trebuie sa suporte expansiunea dinamica a volumelor si LUN-urilor de pana la 2TB. Spatiul astfel alocat suplimentar va fi pus la dispozitia masinilor virtuale ce acceseaza volumele in cauza fara a fi necesara oprirea masinilor virtuale.

Networking:

- Sa permita definirea de zone de securitate la nivel de cluster care sa asigure masinilor virtuale din aceste zone acelasi nivel de securitate (firewall la nivel de hypervisor) indiferent de host-ul pe care ruleaza acestea la un moment dat.
- Solutia va include capabilitatea de definire de switch-uri Ethernet virtuale la nivel de cluster (switch virtual distribuit); acestea vor fi definite si administrate centralizat (dintr-un singur punct) iar configuratia si functiile acestora vor fi automat distribuite tuturor nodurilor din cluster-ul de virtualizare.
- Distributie a traficului de retea prin protocol 802.3ad LACP.

- Monitorizare a traficului de retea prin protocol RSPAN si ERSPAN.
- Suport pentru VXLAN (Virtual Extensible LAN) si SR-IOV (Single Root I/O Virtualization).

Administrare:

- Solutie de management centralizat al resurselor hardware de virtualizare (a masinilor fizice ce alcatuiesc platforma de virtualizare) si al masinilor virtuale create.
- Aplicatia de administrare trebuie sa permita decarcarea automata a patch-urilor si update-urilor si aplicarea acestora atat la nivelul nodurilor de virtualizare cat si a sistemelor de operare din masinile virtuale definite.
- Aplicatia de virtualizare trebuie sa permita managementul salvarilor contextuale (snap-shot) ale masinilor virtuale; o masina virtuala se va putea restaura din orice salvare anterioara.
- Monitorizare in valori numerice si reprezentare grafica a resurselor de procesor, memorie, retea si disc, atat pentru nodurile platformei de virtualizare cat si pentru masinile virtuale definite.
- Monitorizare a starii de functionare si analiza performantei cu functii de auto-invatare si identificare a tendintelor pentru anticiparea congestiilor.
- Administrarea resurselor hardware cu functii de optimizare a utilizarii acestora pentru a asigura o corecta dimensionare a elementelor virtuale si a evita supra-alocarea de resurse hardware.
- Panou de control operational cu analiza cauzelor si generarea de recomandari de remediere.
- Panouri de control personalizabile si ecrane de conformitate operationala
- Praguri dinamice pentru monitorizarea performantei
- Monitorizarea sistemelor de operare in masina virtuala, middleware, aplicatii si baze de date (cel putin pentru Microsoft Windows Server 2008 R2 SP1 Standard Edition, Microsoft SQL Server 2008 R2 Standard.Edition, IIS, .NET, ActiveDirectory si Oracle Database 11g Release 2).
- Functii de alertare si raportare pentru evenimentele si parametrii monitorizati.
- Administrarea schimbarilor, a configuratiei si conformitatii, inclusiv la nivel de sistem de operare in masina virtuala (cel putin pentru Microsoft Windows Server 2008 R2 SP1 Standard Edition, Microsoft SQL Server 2008 R2 Standard.Edition, IIS, .NET, ActiveDirectory si Oracle Database 11g Release 2)
- Cartografiere a dependentelor la nivel de aplicatie (descoperire automata, identificare si versionare, vizualizare a relatiilor de dependenta).

Integrare:

- Sa ofere interfete de programare pentru aplicatii (API) pentru switch-uri virtuale distribuite de alti producatori.

Sa ofere interfete de programarare pentru aplicatii (API) care sa permita producatorilor 3rd party de aplicatii de securitate sa ofere integrarea aplicatiilor lor cu mediul virtual (exemplu: scanare antivirus).

6.6 Sistem de monitorizare

Solutia trebuie sa permita monitorizarea interactiunii utilizatorilor cu aplicatiile.

Acest lucru trebuie realizat prin captura traficului TCP prin metode pasive de tip network sniffing si total neintruzive.
Solutia trebuie sa puna la dispozitie metoda de stocare a acestor informatii capturate, iar managementul acestuia trebuie sa fie automat.
Solutia trebuie sa fie capabila sa captureze si sa retina sesiunile HTTP/HTTPs si sa puna la dispozitie un mecanism de playback prin care sa se poata derula sesiunile capturate.
Solutia trebuie sa fie accesibila intr-o console web, fara instalare de plugin-uri si sa fie suportata minim de Internet Explorer, Mozila, Google Chrome, Opera si Safari
Sa permita crearea de panouri custom cu acces bazat pe roluri
Sa permita autentificarea integrata cu sisteme LDAP versiunea 3, dar cel putin cu urmatoarele: Active Directory, Sun Java Systems Directory Server, OpenLDAP, Novell eDirectory, cu posibilitatea maparii utilizatorilor si a grupurilor din LDAP pe utilizatori si roluri din sistemul de monitorizare
Sa dispuna de un mecanism de alertare bazat pe reguli.
Sa dispuna pentru fiecare tehnologie monitorizata de un set de reguli standard care sa poata fi customizate. De asemenea sa permita crearea de reguli noi
Sa dispuna de un mecanism avansat de notificare si de actiuni la aparitia unei alerte. Sa poata face alertare pe mail catre recipienti alesi in mod dinamic in functie de sistemele afectate, de serviciile de business din care fac parte respectivele sisteme, de perioada din zi (de exemplu alarmele care vin noapte sa fie trimise catre persoana care este de serviciu)
Sa permita executarea de scripturi automate la aparitia alarmelor (de exemplu sa poata elimina automat un proces care consuma 99% CPU si nu are ownerul “oracle”, sau “root”)
Sa permita trimiterea unui trap SNMP la aparitia alarmelor
Managementul Utilizatorilor Finali
Solutia trebuie sa aiba urmatoatele functionalitati
Inregistrarea cererilor end-to-end si a timpilor de retea — Inregistrarea tuturor cererilor si raspunsurilor in aplicatiile Web. Informatia trebuie culeasa inaintea serverelor Web prin mecanisme de captura de trafic fara instalarea de pachete in serverele Web.

Sa poata captura tranzactii reale, sau sa reproduca tranzactii simulate —Sa poata genera tranzactii simulate pentru testarea perfomantei si disponibilitatii aplicatiilor

Sa poata analiza sesiuni individuale de activitate ale utilizatorilor pentru masurarea performantei aplicatiilor web. Sa captureze si sa stocheze sesiuni de lucru utilizator reale; sa reproduca sesiunea capturata din persectiva utilizatorului final

Sa poata monitoriza si alerta cand anumite pagini sunt apelate si sa poata reproduce sesunile derulate pe paginile monitorizate

Sa dispuna de capacitatea de a cauta sesiuni efectuate dupa cuvinte cheie din acestea

Calcularea de SLA-uri pe baza performantei — Formarea unor referinte cu privire la timpii de acces si alertarea utilizatorilor cand aceste valori sunt depasite.

Masuratori detaliate geografic — Monitorizarea timpilor de raspuns defalcat pe locatii geografice, sau alte grupari logice.

Performanta servererlor Web si de aplicatie — Monitorizarea serverelor Web si de aplicatie pentru metrici referitoare la configuratia acestora: CPU, numar de servicii, numar de accese.

Inspectare si analiza de continut — Vizualizarea informatiei exacte afisate in browser-ul utilizatorului final.

Posibilitatea de a tria tranzactiile — Captura si cautare in datele reale ale utilizatorilor pentru a putea vedea ce anume au facut utilizatorii si ce a raspuns sistemul. Posibilitatea de inspectare detaliata a detaliilor tehnice ale modului de interactiune intre utilizator si aplicatie.

Replay de sesiune si tranzactie — Posibilitatea de a reproduce exact activitatea unei sesiuni, sau a unei tranzactii individuale. Posibilitatea de a gasi sesiunile si tranzactiile pe baza filtrarii dupa cuvinte cheie. Mecanismul de reply trebuie sa parcuga pas cu pas paginile vizitate de utilizatori. La fiecare pagina trebuie sa se vada modul in

care utilizatorul a interactionat: ce campuri a completat, ce optiuni a ales, ce link, sau buton a apasat pentru a merge la pasul urmator

Reproducerea problemelor pentru Help-Desk — Posibilitatea de a asambla cu un singur click si de a trimite catre help-desk detaliile unei sesiuni care a dat eroare

Activitatea utilizatorilor trebuie capturata fara impact asupra serverelor – Metoda preferata de captura a sesiunilor utilizatorilor este network sniffing. Doar in acest mod se poate asigura impact zero asupra serverelor web. Metoda de sniffing trebuie sa suporte minim protocoalele: HTTP/HTTPS, TCP, RDP (TCP), SOAP (HTTP).

Functionalitati pentru administrarea bazelor de date

Pentru administrarea bazelor de date, solutia trebuie sa aiba urmatoarele functionalitati:
Sa permita ca procedurile, functiile si pachetele sa poata fi compilate, verificate si depanate

Sa permita modificarea parametrilor de configurare si a optiunilor bazei de date

Sa permita crearea si planificarea de joburi

Sa prezinte sabloane particularizabile pentru proceduri, functii, triggeri si pachete

Buffer de undo/redo, sintaxa colorata, facilitate de scriere type-ahead, liste de selectie pentru coloane sau proceduri din pachete, localizarea rapida a erorilor si afisarea lor intr-o semifereastra, localizarea rapida a componentelor din pachete (prin afisarea lor intr-o fereastra din stanga ferestrei de editare), posibilitatea de salvare sau recuperare pe/de pe disc in formate variate cum ar fi HTML, Excel, statement-uri INSERT,

Sa permita o administare completa a securitatii din baza de date prin crearea, modificarea, stergerea utilizatorilor, rolurilor si profilurilor

Sa permita vizualizarea si administrarea tablespace-urilor, fisierelor redolog, segmentelor rollback, fisierelor de control pentru managementul spatiului

Sa contina editoare de scripturi SQL, proceduri, functii, trigere etc, care sa aiba functii de tip “make” si “strip” de portare a frazelor sql direct din si catre alte aplicatii

Sa poata crea si modifica rapid obiectele din baza de date, sa poata vizualiza dependintele dintre obiectele schemei, sa poata realiza comparari si afisari de rapoarte pe schema si pe obiectele din ea, precum si diagrame cu obiectele din schema

Sa permita cautarea dupa criterii diverse a obiectelor din baza de date

Sa permita compararea de scheme, fisiere de cod

Sa permita formatarea customizata a codului pentru o mai buna lizibilitate, sa permita criptarea codului stocat in baza de date

Sa contina o colectie completa de „code snipets” (mici blocuri de cod reutilizabile) pentru majoritatea functiilor bazei de date

Sa includa si un modul specializat de debug al codului pl/sql care sa faciliteze crearea unor asa zise view-uri, imbunatatind seminificativ timpul de detectare a erorilor.

Sa detecteze erorile de logica in programare, sa efectueze rulari pas cu pas si sa faciliteze rezolvarea problemelor fara scrierea de cod suplimentar pentru detectarea portiunilor de cod in dubiu. Acest lucru trebuie realizat prin intermediul unui modul specializat de tip expert de cod pl/sql care, pe baza unui set de reguli sa sugereze imbunatatiri ale metodologiei de programare.

Prin intermediul lui sa se poate urmari evolutia unei proceduri sau functii (chiar apelata si din exterior) fara

inserare de cod suplimentar

Sa contina wizard-uri detaliate pentru operatiunile de import, export, data pump si sqlload

Sa permita exportul ad-hoc al rezultatului unui query in formatele uzuale (csv, text, excel, etc.)

Sa contina un modul cu functionalitate de Group Policy care sa adauge un strat intermediar peste securitatea nativa a bazei de date, care sa permita o mai buna gestiune a accesului utilizatorilor la functionalitatile produsului de administrare.

Sa permita lucrul in echipa cu functionalitati de versionare a codului si functii “check-in” si “check-out”

Functionalitati pentru diagnosticarea performantelor in timp real

Pentru diagnosticarea performantelor in timp real, solutia trebuie sa aiba urmatoarele functionalitati
produsul trebuie sa realizeze diagnosticul activitatii sistemului in timp real

sa permita conectarea din aceeasi consola la multiple instante de baze de date, indiferent de versiunea acestora

sa aiba o interfata vizuala, respectiv o harta a arhitecturii bazei de date din care sa se poata vizualiza exact componentele sale precum si fluxul de date intre acestea

interfata vizuala sa fie insotita de explicatii privind fiecare element al arhitecturii bazei de date cu acces rapid si link-uri catre manuale electronice la topic-ul care explica exact elementul din arhitectura bazei de date pe care s-a dat click

sa permita executarea unei aplicatii pe client in momentul aparitiei unei alarme

sa permita diagnosticul atat al bazei de date cat si al sistemului de operare de pe serverul de baza de date

sa identifice vizual gatuirile la nivel de sistem avand facilitati de inspectare detaliata (drill down)

sa notifice administratorul de baze de date prin intermediul alarmelor vizuale, auditive, mail sau pager cand un anumit prag critic este depasit (threshold). Sa permita customizarea acestor praguri de alertare, precum si configurarea lor automata in functie de activitatea bazei date printr-un proces de calibrare.

sa permita trimiterea selectiva de alerte, pe baza de reguli, inclusiv doar a alertelor care nu au fost detectate de administrator (de exemplu s-au petrecut noaptea sau in pauza)

sa permita un istoric al incidentelor cu posibilitaea reproducerii exacte a activitatii din momentul producerii lor. Inregistrarea activitatii bazei de date in scopul reproducerii se va face pe o perioada de mai multe zile in functie de spatiul alocat pentru aceasta

administratorul sa poata in orice moment, in mod vizual sa faca „replay” la activitatea din baza de date pentru a vizualiza cu exactitate situatia in care a fost generata o alerta

solutia sa fie disponibila pentru cele mai cunoscute platforme de baze de date si sa permita monitorizarea acestor platforme din aceeasi consola

Solutia trebuie sa suporte baze de date de tip cluster

sa permita diagnosticarea unui cluster atat la nivelul unui nod individual, cat si la nivelul clusterului ca entitate

sa permita vizualizarea incarcarii interconect a latentei si overheadului cauzate de cluster

sa permita diagnosticarea si alertarea cu privire la subsistemul I/O

Sa permita vizualizare alert log-ului

Sa contina un modul de diagnostic predictiv care sa detecteze inconsistentele in trendul performantei frazelor SQL

Sa suporte ASM (in cazul Oracle)

Functionalitati pentru optimizarea instructiunilor SQL

Pentru optimizarea instructiunilor SQL, solutia trebuie sa aiba urmatoarele functionalitati.

Sa detecteze instructiunile SQL cu probleme de performanta, direct din obiecte stocate in baza de date (proceduri, vederi etc.) sau din fisiere sursa fara a necesita executia lor; in plus permite si detectarea instructiunilor SQL dinamice (create la momentul executiei)

Sa detecteze instructiunile SQL cu probleme de performanta direct din datele capturate de modulul de analiza de performanta.

Sa ofere posibilitatea de a scana, gasi si optimiza instructiunile ineficiente

Sa permita vizualizarea in detaliu planurile de executie ale instructiunilor SQL

Sa gaseasca automat instructiunile SQL alternative - instructiuni cu sintaxa diferita dar echivalente semantic (produc exact acelasi set de rezultate)

Sa execute automat scenariile asociate cu originalul si cu alternativele gasite in vederea colectarii de statistici privind executia lor

Sa permita compararea statisticilor aferente si alegerea automata a celui mai bun scenariu.

Sa permita utilizatorului sa decida intre scenariile alternative, varianta pe care o considera optima

Sa se integreze cu un modul de Benchmarking pentru teste de scalabilitate

Sa aiba facilitati de generare alternative de indecsi pentru o anumita instructiune SQL in relatie cu tabelele referite, sa permita simularea lor si alegerea celor mai bune variante

Sa permita crearea si gestionarea de planuri de executie (outlines)

Functionalitati pentru simularea accesului si testarea bazei de date

Pentru simularea accesului si testarea bazei de date, solutia trebuie sa aiba urmatoarele functionalitati

Sa permita executia unor teste standard in industrie (AS3AP, Scalable Hardware , TPC-B, TPC-C, TPC-D, TCP-H)

Sa permita crearea propriilor scenarii de test prin introducerea frazelor SQL

Sa permita capturarea frazelor sql direct din fisierele sql trace ale bazei de date, putand, in acest fel, reproduce in mod exact activitatea din baza de date

Pentru simularea frazelor sql, produsul sa aiba dictionare detaliate (nume, coduri postale, localitati, etc.), precum si functii speciale de generare aleatoare si/sau unice de valori (numerice, de tip data, de tip text). In acest mod se va evita repetarea la nesfarsit a unei singure fraze sql (lucru nerelevant pentru analiza), sau un efort prea mare de concepere a scenariului de test

Sa permita combinarea tuturor acestor scenarii de test

Sa permita analiza scenariilor executate si culegerea de statistici de tipul „transaction/second”, „response time”, etc

Sa permita executia scenariilor de test in paralel cu multiple conexiuni la baza de date, in acest fel simulandu-se activitatea concurenta a utilizatorilor

Sa permita folosirea de agenti comandati de la o consola centralizata pentru a putea balansa numarul de

conexiuni deschise statiilor client. Adica, daca se doreste simulare cu 250 de useri concurenti, sa se poata face de pe 10 statii de lucru, fiecare cu cate 40 de sesiuni deschise la baza de date

Sa permita aplicabilitate la baze de date Oracle, SQL Server, DB2, Sybase, precum si orice baza de date ODBC compliant

Managementul echipamentelor de retea

Solutia trebuie sa ofere monitorizarea, controlul si diagnosticarea echipamentelor de retea (daca este cazul), serverelor, sistemelor de operare si a altor echipamente de infrastructura IT. Solutia va trebui sa gestioneze infrastructura ca si suport pentru aplicatiile critice, din fiecare perspectiva, inclusiv vizualizarea nivelelor de servicii ale business-ului.

Solutia trebuie sa poata captura starea intregii retele prin monitorizarea in timp real a parametrilor functionali, alertarea asupra problemelor, raportarea detaliata si sa ofere un real suport pentru personalul IT in vederea remedierii problemelor de latine de banda, conectivitate, performanta a retelei si aplicatiilor.

Solutia trebuie sa aiba urmatoarele functionalitati:

Alertare avansata – sa notifice via e-mail sau SMS cand performanta se degradeaza, permitand remedierea problemelor inainte sa impacteze asupra experientei utilizator. Alertele trebuie sa poata fi configurabile, sa suporte conditii multiple si sa se raporteze la un baseline de performanta particularizat de aplicatie pentru mediul informatic pe care il monitorizeaza. Sa identifice si sa elimine alertele fals - pozitive

Monitorizarea aplicatiilor – sa furnizeze vizibilitate in adancime a proceselor ce ruleaza si contoarelor de performanta pentru aplicatiile critice, serviciile de retea si aplicatiile web

Remedierea automata – sa poata lua automat masuri de restaurare a serviciilor, inclusiv restartarea aplicatiilor si serviciilor Windows, sau sa restarteze serverele

Monitorizare de cloud – sa poata gestiona si monitoriza atat infrastructura locala, cat si mediile de cloud computing de la distanta, in aceeasi interfata

Suport cross-platform – sa furnizeze monitorizare neintruziva si fara incarcare asupra platformelor Windows, Linux sau Mac. In cadrul monitorizarii, sa poata comunica informatiile centrului de control, iar apoi sa livreze serviciile cerute

Monitorizare in timp real – sa furnizeze monitorizare in timp real si colectare de date, inclusiv in timpul procesului de depanare. Sa monitorizeze in timp real indicatorii de performanta de pe routere, hub-uri, switch-uri, servere si aplicatii

Interfata de lucru integrata – sa ofere o interfata web compatibila cu browser-ele comune, in interiorul careia sa fie disponibile toate informatiile critice, gatuirile de retea si alertele de performanta. De asemenea, sa permita efectuarea de setari aplicatiei de monitorizare

Monitorizare wireless – sa poata monitoriza retelele wireless. Sa centralizeze managementul retelelor wireless distribuite, prin aplicarea de configuratii comune si afisarea centralizata a datelor

Deployment facil – sa permita autodescoperire de echipamente, recunoastere de echipamente descoperite si sa aiba capacitatea de a configura automat setul potrivit de instrumente de monitorizare pentru fiecare categorie de echipamente descoperite

Management de log-uri – sa poata colecta, analiza, alerta, raporta si arhiva loguri de evenimente de pe gazdele Windows, syslog de pe platformele UNIX/Linux si echipamente de retea, precum si loguri de aplicatie de pe serverele IIS si MS SQL

Suport pentru echipamente mobile – sa existe posibilitatea de a livra rapoarte si date d emonitorizare catre echipamente mobile

“Dashboard” de monitorizare – sa furnizeze o interfata de vizualizare tip dashboard, care sa contina un set cuprinzator de date sumarizate privind performanta retelei si a echipamentelor. “Dashboard-ul” trebuie sa fie

usor de customizat pentru a raspunde cerintelor organizatiei

Monitorizarea fluxului de retea – sa permita vizualizarea si analiza in timp real a traficului de retea. Sa stocheze datele de flux in vederea raportarii istorice si optimizarii capacitatii de retea

Unelte de diagnostic – sa includa sau sa furnizeze suport pentru un set cuprinzator si centralizat de unelte de diagnosticare: utilitare de ping, mappere de porturi, managere de configuratii echipamente, generatoare de trafic etc.

Suport de tip "remote office" – sa furnizeze conectivitate securizata cu site-uri remote

Rapoarte asupra datelor colectate – sa permita generarea de rapoarte pentru toate datele colectate. Rapoartele trebuie sa poata fi exportate in formatele uzuale, tiparite sau expediate prin e-mail. Rapoartele trebuie sa poata fi generate ad-hoc sau un baza unui calendar. Prin rapoartele built-in, sa faca posibila analiza tendintelor si planificarea capacitatii peste timp, in vederea anticiparii cerintelor de viitor

Acces bazat pe roluri – sa permita configurarea de conturi utilizator mapate pe roluri administrative

Backup de configuratii – sa dispuna de capacitatea de a realiza backup de configuratie pentru routere si switch-uri

Suport pentru tehnologiile standard – sa suporte analiza de trafic personalizata pentru tehnologiile standard de pe piata, in special CISCO NetFlow si Juniper J-Flow. Sa ofere suport pentru: WMI, NetFlow, sFlow, J-Flow, SNMP

Managementul personalizat al monitorizarii – sa permita setarea de politici de monitorizare aplicabile pe categorii de echipamente

SNMP enablement – sa activeze si sa configureze in mod automat SNMP pe echipamente in vederea includerii rapide in procesul de monitorizare a unor range-uri mari de echipamente

Suport pentru mediile virtualizate – sa descopere automat host-urile de virtualizare ESX si masinile virtuale gazduite de acestea, si sa furnizeze statistici cheie din interiorul acestora: starea curenta, utilizare CPU / memorie / disc, precum si traficul pe interfete

Network mapping – Sa permita crearea de harti de retea actualizate in timp real

Pentru managementul infrastructurii de monitorizare si securitate se va folosi si propune o statie de lucru dedicata, care sa poata gestiona in conditii de securitate informatia vehiculata.

6.7 Serviciu securizat de management al cererilor si solicitarilor din partea utilizatorilor

Serviciul securizat de management al cererilor si solicitarilor din partea utilizatorilor contribuie la acoperirea necesitatilor operationale ale Beneficiarului, rezultate din reglementarile care definesc cadrul de organizare si functionare, in concordanta cu strategia adoptata.
Acest serviciu joaca rol de suport pentru alte servicii/module din cadrul sistemului si este un instrument de management al documentelor si workflow securizat, ce asigura circulatia documentelor conform fluxurilor definite.
Serviciul securizat de management al cererilor si solicitarilor din partea utilizatorilor va deservi entitatile organizationale implicate in activitatile de verificare, avizare si control in cadrul procedurilor de achizitie publica desfasurate prin sistem. Acest serviciu se va integra cu Serviciul pentru gestiunea fiselor de date din cadrul SEAP.
Serviciul securizat de management al cererilor si solicitarilor trebuie sa permita validarea mai multor tipuri de documente care tin de procedura de achizitie publica (), documente incarcate de catre autoritatile contractante/ ofertanti in sistem. Acest serviciu va oferi trasabilitatea documentelor si a actiunilor utilizatorilor in sistem.
Documentele vor trebui repartizate pentru verificare printr-un mecanism de repartizare automat si transparent pentru utilizator. De asemenea, serviciul trebuie sa permita definirea mai multor tipuri de utilizatori, functie de rolurile detinute de acestia in cadrul procesului de validare: utilizatori cu rol de verificare, utilizatori cu rol de avizare, utilizatori cu rol de supervizare/control.

Serviciul propus trebuie sa permita configurarea de termene pe fluxurile electronice de avizare, conform legislatiei in vigoare. Astfel, serviciul va trebui sa ofere posibilitatea de configurare si reconfigurare facila de termene, direct din interfata serviciului, atat pentru fluxuri cat si pentru activitatile acestuia.
Serviciul trebuie sa permita monitorizarea fluxurilor de avizare pe baza unui rol, care poate fi acordat atat utilizatorilor cu functie de supervizare/control – care nu sunt neaparat implicati in fluxurile electronice de avizare, cat si utilizatorilor cu rol de verificare sau avizare. Monitorizarea fluxurilor va oferi utilizatorilor informatii despre unul sau mai multe fluxuri active/finalizate intr-un anumit interval de timp. Pentru fiecare instanta de flux se va putea verifica in detaliu traseul documentului, rezolutiile acordate, timpul petrecut in fiecare pas din flux, iar in cazul depasirii termenului pe flux/activitate, acest lucru va fi marcat distinct.
Managerii trebuie sa poata monitoriza activitatea subordonatilor pe fluxurile de documente pe care acestia sunt implicati si vor putea monitoriza gradul de incarcare al fiecarui subaltern la un moment dat.

6.7.1 Cerinte generale

a) Toată interfaţa sistemului pentru toate modulele va fi în limba română. Toate ecranele de introducere date, administrare parametrii sistem, nomenclatoare, liste etc vor fi în limba română. De asemenea, manualele de utilizare, administrare si instalare vor fi in limba romana, iar instruirea se va desfasura tot in limba romana.
b) Serviciul trebuie sa asigure gestiunea independenta a diverselor entitati organizatorice, a fluxurilor interne de lucru, a documentelor si categoriilor de documente specifice, a utilizatorilor si rolurilor asociate, a bibliotecilor si arhivei electronice.
c) Serviciul trebuie sa fie dezvoltat in tehnologie Internet (web based). Nu se vor agrea solutii de tip client server sau distribuite pe statii de lucru (web enabled). Accesul utilizatorilor din interiorul institutiei trebuie sa se faca prin intermediul unui WEB browser.
d) Serviciul trebuie sa permita lucrul cu documente clasificate, conform legislatiei in vigoare (Legea 182 din 2002).
e) Serviciul trebuie sa ofere „Help” contextual in limba romana.
f) Fluxurile de lucru trebuie sa fie configurate prin intermediul unei interfete grafice web-based fara utilizarea de limbaje de scripting.
g) Serviciul propus trebuie să dispună de un mecanism propriu de semnare electronică a documentelor (atât metadate cât şi fişiere) direct din interfaţa web. Acest mecanism trebuie să permită de asemenea şi verificarea validităţii semnăturii electronice direct din interfaţa web pentru datele (metadate şi/sau fişiere) semnate electronic.
h) Serviciul propus trebuie să ofere facilităţi incorporate de management al documentelor şi conţinutului care să permită stocarea fişierelor în orice format electronic. Principalele funcţionalităţi care trebuie oferite sunt:
    1) Suport pentru stocarea conținutului în unul sau mai multe depozite de documente
    2) Acces controlat la conținutul documentelor
    3) Conținut structurat și nestructurat
    4) Distribuția conținutului pe noduri multiple, care să lucreze în cluster
    5) Definirea ierarhicăde tipuri de noduri cu metadate/proprietăți specifice
    6) Tranzacționalitatea operațiilor pe baza de date
    7) Funcționalitate pentru acces concurențial și exclusiv la conținut, de tip check in/check out
    8) Versionare de conținut în cadrul depozitului de documente
    9) Indexarea și reindexarea conținutului documentelor
    10) Căutare simplă și complexă în conținutul de tip text
    11) Import de fișiere multiple
    12) Suport pentru standardul WebDAV
    13) Interogări Xpath și SQL

6.7.2 Cerinte tehnice

In ceea ce priveste ergonomia sistemului se solicita respectarea urmatoarelor cerinte:

a) Interfata cu utilizatorii trebuie sa fie ergonomica, functionala si facila in utilizare
b) Aplicatia va oferi un sistem de help in limba romana, separat pentru administratori si utilizatori obisnuiti
c) Aplicatia trebuie sa aiba interfata in limba romana
d) Ecranele vor fi proiectate astfel incat sa fie optim utilizate la o rezolutie de minim 1024x768 pixeli

e) Interfata trebuie sa asiste utilizatorii la introducerea datelor prin implementarea de valori implicite, reguli de validare si mesaje sugestive in caz de eroare.

Din punct de vedere tehnologic, se impune utilizarea unei platforme deschise, care sa asigure urmatoarele caracteristici:

a) Indepedenta de platforme hardware (RISC, CISC)
b) Independenta de platforme software de baza: sistem de operare, sistem de baze de date, server de aplicatie
c) Scalabilitate (orizontala si verticala)
d) Flexibilitate
e) Extensibilitate facila
f) Suport din partea producatorilor majori de tehnologie
g) Suport pentru arhitecturi distribuite, organizate multi-strat
h) Integrare cu sisteme existente

Aplicatiile trebuie sa fie realizate in conformitate cu urmatoarele standarde:

a) W3C – Worl Wide Web Consortium
    1. HTML
    2. XML
    3. XSL
    4. XML Schema
    5. Web Services
b) J2EE - Java 2 Enterprise Edition
    1. EJB - Enteprise Java Beans
    2. JSP - Java Server Pages
    3. JNDI - Java Naming and Directory Interface
    4. JDBC - Java Database Connectivity
    5. JCA - Java Connector Architecture
    6. JTA - Java Transaction API
    7. JavaMail
    8. JavaBeans
    9. JMS - Java Message Service
    10. Java Servlet Specification
    11. JSR 170
c) PKI – Public Key Infrastructure
    1. PKCS#1 RSA Encryption Standard (512, 1.024, 2.048 bit)
    2. PKCS#7 Cryptographic Message Syntax Standard
    3. PKCS#11 Smart card and Token Standard
    4. PKCS#12 Personal Information Exchange Syntax Standard
    5. X.509 Version 2 CRL
    6. X.509 Version 3
    7. LDAP
    8. RSA for encryption standard
    9. SHA – 1 and MD 5 hashing/digest standards
    10. PadES - PDF Advanced Electronic Signatures
d) WfMC – Workflow Management Coalition
    1. WfMC-TC-1003 - Workflow Reference Model
    2. WfMC-TC-1001 - Terminology and Glossary
    3. WfMC-TC-10160-P - Process Definition Meta-Model
e) SQL – Structured Query Language
    1. SQL 92
    2. SQL 99
    3. SQL 2003

6.7.3 Caracteristici avansate de securitate

Dat fiind caracterul senzitiv al informatiilor vehiculate in interiorul institutiei, dar si in comunicarile cu aparatul central, sistemul de management securizat de documente si fluxuri de lucru electronice din trebuie sa asigure un set de functionalitati avansate de securizare a lucrului cu acest tip de informatii. Astfel, se doreste ca sistemul sa fie capabil sa ofere:

a) Autentificare pe baza de elemente avansate de securitate (certificat digital, echipamente de tip token)
b) Utilizarea semnaturii digitale la adaugarea si modificarea documentelor, la luarea deciziilor asupra documentelor electronice din sistem, precum si la depunerea documentelor in arhiva electronica, in scopul garantarii integritatii si non-repudierii informatiilor
c) Verificarea semnaturii de catre sistem, pe baza recipiselor si a datelor mentinute in sistem
d) Controlul strict al accesului la documente, indiferent de starea acestora. Se doreste folosirea unui set cat mai larg de criterii de acordare a accesului (in functie de tipul documentelor, tipul de operatie, starea documentului, etc)
e) Monitorizarea stricta a accesului la documente si jurnalizarea operatiilor
f) Asigura conformitate cu standardele PKCS #1, PKCS #7, PKCS #11
g) Operatiunile implicand semnarea si criptarea se vor realiza utilizand certificate digitale
h) Posibilitatea criptarii simetrice cu urmatorii algoritmi: DES, 3DES, RC4, RC6
i) Certificatele digitale ale utilizatorilor vor putea fi stocate pe dispozitive de token USB conforme cu standardul FIPS 140-2 level 2
j) Operatiunile criptografice care implica utilizarea cheii private se vor desfasura numai pe dispozitive de tip token USB conforme cu standardul FIPS 140-2 level 2
k) Asigurarea legaturii cu serviciul de marcare temporala de la nivelul aparatului central conform RFC 3161
l) Folosirea unor certificate digitale separate pentru operatiunile de criptare si semnare
m) Autentificarea utilizatorilor in sistem se va realiza pe baza de nume si parola, precum si de certificate emise de autoritatea de certificare de la nivelul aparatului central, cu garantarea validitatii starii certificatelor digitale la acel moment de timp, accesand serviciul de validare OCSP (RFC 2560)
n) Compatibilitate cu standardul LDAP v3
o) Comunicatia intre partea client a sub-sistemului si partea server trebuie sa fie garantata din punct de vedere al confidentialitatii in orice moment de timp. Pentru comunicatia online este obligatoriu sa se asigure conexiune de tip HTTPS (SSL 128 biti) cu autentificare reciproca
p) La fiecare operatiune senzitiva, de aprobare sau avizare pe fluxurile de documente sistemul va solicita utilizatorului semnarea formularului de date.

Se va asigura integrare cu solutia de Autoritate de Certificare utilizata in cadrul proiectului.

6.7.4 Managementul ciclului de viata al documentelor

Pentru gestionarea ciclului de viata al documentelor electronice va trebui sa ofere urmatoarele functionalitati:

a) Adaugarea manuala de documente in orice format electronic impreuna cu un set de metadate standard (nume document, tip, data creare, cuvinte cheie, etc)si cu un set de metadate specifice fiecarei categorii de document
b) Adaugarea de documente in sistem prin preluarea automata de documente de la alte servicii sau subsisteme IT care deservesc sistemul de achizitii publice. Documentele vor putea fi preluate de la alte servicii sau subsisteme cu tot cu anexe si metadate specifice categoriei de document
c) Posibilitatea de a popula metadatele fie manual, fie automat la preluarea unui document de la alt serviciu, fie la finalizarea unui flux parcurs de document
d) Organizarea metadatelor specifice fiecarei categorii de document, pe sectiuni
e) Acordarea drepturilor de acces per metadata sau sectiuni de metadate
f) Stocarea tuturor documentelor interne în format electronic într-un depozit (repository) de documentecu o structură ce asigură evidenţierea versiunilor intermediare de lucru, împreună cu atributele lor, astfel încât să se poată găsi repede informaţia necesară
g) Posibilitatea de a clona tipurile de document, pastrand integral structura acestuia, inclusiv structura formularului asociat
h) Exportul formularelor in format PDF

i) Versionarea automata a documentelor la orice modificare, cu pastrarea si vizualizarea versiunilor anterioare. Serviciul trebuie sa permita si versionarea metadatelor specifice fiecarei categorii de document.

j) Pentru fiecare document, trebuie sa se poata adauga adnotari de tip rich text. Unui document ii pot fi adaugate oricate comentarii atat de catre utilizatorul care a creat documentul, cat si de utilizatorii care au primit documentul pe flux, sau au fost solicitati pentru lucru colaborativ la respectivul document etc, in general de toti utilizatorii care au drept de editare a documentului

k) Pentru fiecare document, trebuie sa se poata adauga cuvinte cheie. Cuvintele cheie definesc un set de cuvinte reprezentative asociate unui document, pentru ca ulterior sa ajute la cautarea facila a documentului. Unui document i se vor putea adauga oricate cuvinte cheie din urmatoarele doua tipuri: cuvinte cheie personale, introduse fara restrictii de fiecare utilizator in parte, respectiv cuvinte cheie globale, care reprezinta o lista arborescenta de cuvinte cheie predefinite de catre un administrator, lista din care utilizatorul poate alege.

l) Pentru fiecare document trebuie sa se poata stabili nivelul de clasificare.

m) Pentru fiecare categorie de document trebuie sa se poata defini termenul de pastrare, conform informatiilor din nomenclatorul arhivistic.

n) Semnarea digitala a versiunii curente a documentelor si posibilitatea de verificare si validare a semnaturii de catre alti utilizatori. La semnare, sistemul va genera o recipisa electronica, ce va putea fi stocata in aplicatie sau pastrata in afara ei. Recipisa va putea fi folosita pentru verificarea semnaturii in cazul unor contestatii.

o) Posibilitatea de a vizualiza documente in formate proprietare fara a fi necesara instalarea de aplicatii suplimentare. Astfel de formate includ: Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Adobe Acrobat, fisiere imagine in formatele consacrate (jpg, gif, tif, bmp), fisiere HTML

p) Integrare cu suite de aplicatii Microsoft Office (Word, Excel, Powerpoint) care sa permita salvarea directa in sistem a documentelor editate cu aceasta suita

q) Posibilitatea de a organiza documentele pe categorii/taxonomii de documente in scopul regasirii facile a informatiilor prin intermediul explorarii ieharhice multi-criteriale

r) Posibilitatea de a pastra documente in spatiu de lucru privat sau de a le publica in spatu public.

s) Posibilitatea de a organiza documentele in dosare (grupuri de documente), cu pastrarea tuturor functionalitatilor specifice conceptului de document si la nivelul conceptului de dosar

t) Posibilitatea de a copia documentele, iar noul document (copia) trebuie sa pastreze o legatura catre original

u) Posibilitatea de indexa automat continutul documentelor in format text cu posibilitatea de cauta documente dupa continut

v) Suport pentru gruparea ad-hoc a documentelor in asociatii de mai multe documente si stabilirea de corespondente intre doua grupari de documente

w) Sistemul trebuie sa fie capabil sa ofere fiecarui utilizator un spatiu privat de lucru, in care acesta sa-si pastreze si organizeze documentele. Organizarea documentelor trebuie sa se faca sub forma de directoare si subdirectoare de documente. In cadrul structurii de directoare vor putea fi efectuate urmatoarele operatii: adaugare, redenumire, stergere, clonare, mutare director, adaugare/stergere/mutare document intr-un director.

x) Sistemul trebuie sa ofere suport pentru desfasurarea activitatilor intr-o schema multi-structura, fiecare structura avand posibilitatea de a-si gestiona separat utilizatori si roluri, fluxuri de lucru, categorii de documente, bibloteci si arhive de documente.

y) Cautarea simpla (set de criterii redus) sau cautare complexa (set de criterii extins). Caracteristici ale cautarii:

1. Cautarea sa se faca atat in metadate standard, in metadate specifice categoriei de document, cat si in continut
2. Sa se poata folosi expresii regulate
3. Sa se poata salva criteriile de cautare
4. Rezultatele sa poata fi salvate in format PDF

z) Posibilitatea ca anumite informatii din metadatele specifice sa fie transmise catre alte servicii la aparitia unor evenimente (de exemplu la acordarea unei rezolutii pe un flux)

aa) Sistemul trebuie sa se integreze cu echipamente de scanare/indexare a documentelor in format hartie, cu posibilitatea de preluare automata a documentelor in mod individual sau in sistem batch. Fisierele scanate din interfaţa de scanare trebuie să poată fi de tip multi-pagina TIFF. La scanare trebuie sa fie posibila definirea de

metadate care se vor regasi pe documentele din sistem. Subsistemul de captura trebuie sa permita procesare automata OCR si recunoastere de coduri de bare.

6.7.5 Lucrul in comun pe documente

Sistemul de document management trebuie sa puna la dispozitie diferite tipuri de lucru in comun cu documentele electronice. Astfel, sunt avute in vedere urmatoarele tipuri de colaborare in elaborarea documentelor

a) Colaborare formala: in acest caz, etapele prin care trece un document (verificat, avizat, aprobat) sunt definite unor fluxuri electronice de lucru, conform unor proceduri de lucru prin configurarea fiecarui pas prin care un document trece, a actorilor implicati si a drepturilor asociate pe fiecare pas, precum si a conditiilor de trazitie intre pasi. La executia fluxului, fiecare utilizator va executa sarcina alocata si va trimite documentul/documentele catre pasul urmator conform regulilor de tranzitie definite (sistemul va afisa automat destinatiile posibile in functie de configurarea fluxului). Trebuie sa fie posibila configurarea fluxului astfel incat in anumiti pasi sa se impuna semnarea digitala a documentului si a deciziilor luate asupra documentului in acel pas.
b) Colaborare informala: Posibilitatea de a partaja documentele:
    1. direct intre utilizatori, prin publicarea unui document/set de documente catre o lista nominala de utilizatori pentru lucru colaborativ.
        - La publicare sa se poata defini fie un mesaj de lucru comun pentru intreaga lista, fie mesaje individuale pentru fiecare utilizator.
        - Pentru lucrul simultan pe documente trebuie implementat un mecanism de acces exclusiv la document, de tip blocare/deblocare.
        - Odata publicat un document, utilizatorul care a publicat documentul trebuie sa poata vedea stadiul lucrului pentru fiecare utilizator si poate retrage, in orice moment, documentul de la publicare.
        - Documentele primite in colaborare de catre un utilizator trebuie sa fie evidentiate in prima pagina a aplicatiei, astfel incat acesta sa aiba acces rapid si control asupra documentelorprimite in lucru.
        - Documentele trimise in colaborare catre alti utilizatori trebuie sa fie evidentiate in prima pagina a aplicatiei, astfel incat initiatorul colaborarii sa poata vedea stadiul lucrului pentru fiecare document in parte
    2. prin intermediul unei biblioteci de lucru, cu configurarea drepturilor de access. Biblioteca trebuie sa poata fi organizata pe sectiuni si subsectiuni, iar drepturile de access trebuie controlate la nivel de tip de operatie pe (sub)sectiune a bibliotecii. Documente trebuie sa poata fi vizualizate, preluate din biblioteca pentru modificare, pastrand o urma in biblioteca, respectiv sa poata fi retrase complet din biblioteca conform drepturilor alocate pentru fiecare utilizator.

6.7.6 Managementul fluxurilor de lucru

In cazul colaborarii formale intre utilizatori, prin intermediul fluxurilor electronice de lucru, se solicita urmatoarele functionalitati:

a) Definirea metadatelor generale ale fluxurilor electronice (nume, perioada de valabilitate, durata maxima de executie, etc)
b) Definire setului de activitati ce fac parte dintr-un proces si metadatelor asociate (nume, tip, durata maxima, roluri asociate, drepturi de acces si prelucrare asupra documentelor asociate respectivei activitati)
c) In fiecare activitate trebuie sa se poata acorda un set de decizii (rezolutii) configurabile la nivel administrativ. Aceste decizii trebuie sa poate fi insotite de comentarii in mod text sau de comentarii vocale (prin inregistrarea de mesaje). Trebuie sa existe posibilitatea de a configura pentru fiecare activitate daca rezolutiile sunt semnate digital.
d) In orice activitate de pe flux sa se poata vizualiza, tipari la imprimanta direct din interfata aplicatiei si exporta in format .pdf atat lista rezolutiilor acordate pana in acel pas de catre utilizatori, cat si diferentele aparute intre versiunile documentului care a fost rezolutionat pe flux.
e) Lista rezolutiilor de pe flux exportata in format .pdf trebuie certificata de catre sistem ca fiind autentica, ori prin semnatura digitala atasata, ori prin watermark pe paginile fisierului exportat, configurabil din interfata de administrare.
f) Pe langa administrator, trebuie ca si initiatorul unui flux sa poata configura urmatorii parametrii: timpul maxim de executie al intregului proces, timpul maxim de executie al fiecarei activitati

g) Sistemul trebuie sa poata fi configurat astfel incat sa se poata acorda termene pe activitati sau seturi de activitati in orice pas din flux si simultan, mai multe termene pe un flux.
h) Sistemul trebuie sa permita definirea tranzitiilor intre activitati si a setului de conditii care trebuie indeplinit pentru executia fiecarei tranzitii. Acest set de conditii trebuie sa includa criterii precum rolurile expeditor, rolurile destinatar, tipul documentelor, rezolutii acordate, etc. De asemenea, pentru a asigura o cat mai mare flexibilitate a tranzitiilor, sistemul trebuie sa ofere o paleta larga de posibilitati de configurare pentru fiecare dintre ele. Printre configurarile posibile trebuie sa se numere:
    1. posibilitatea de a executa simultan mai multe tranzitii dintr-o singura activitate catre activitati diferite si posibilatea de a uni un set de tranzitii intr-una singura
    2. posibilitatea trimiterii mesajului doar utilizatorilor din acelasi grup de lucru cu expeditorul
    3. posibilitatea trimiterii mesajului catre toti utilizatorii ce au rolul destinatar ales
    4. posibilitatea trimiterii mesajului numai catre autorul documentului ce parcurge fluxul
    5. posibilitatea trimiterii mesajului numai catre expeditorul mesajului primit
    6. posibilitatea trimiterii mesajului catre toti destinatarii posibili
    7. posibilitatea crearii dependintei dintre activitatea pentru care se defineste tranzitia si o alta activitate a procesului curent
    8. posibilitatea trimiterii mesajului pe o anumita ierarhie, catre superior sau catre subordonat.
    9. posibilitatea de a conditiona tranzitia in functie de valorile unui campuri dintr-un formular asociat documente
    10. posibilitatea notificarii prin e-mail a sefului direct sau a tuturor sefilor ierarhici pe o ierarhie aleasa.
i) Sistemul va oferi suport pentru modificarea la runtime a fluxurilor de documente electronice, prin modificarea rolurilor implicate, durata activitatilor sau conditiile de tranzitie
j) Sistemul va oferi suport pentru vizualizarea fluxurilor electronice finalizate sau a celor aflate in lucru, cu precizarea punctelor in care se gaseste un flux la un moment dat si a pasilor anterior parcursi
k) Fluxul trebuie sa poata fi configurat sa faca in mod automat copii ale documentului la parasirea unui activitati din flux, documentul intrand in proprietatea celui care a efectuat acea activitate
l) Un flux electronic trebuie sa poata fi configurat astfel incat la finalizarea unei instante documentul sa intre automat fie in proprietatea initiatorului fluxului, fie in biblioteca, cu alegerea sectiunii in care se va depozita documentul.
m) Sistemul trebuie sa ofere suport pentru definirea fluxurilor prin intermediul interfetei grafice de tip web
n) Sistemul trebuie sa permita ca din orice pas de pe flux documentul sa poata fi trimis unor utilizatori din afara fluxului, in colaborare.
o) Sistemul trebuie sa ofere suport pentru clonarea fluxurilor in vederea crearii de fluxuri noi pe baza celor deja definite in sistem
p) Sistemul va oferi suport pentru monitorizarea gradului de incarcare a utilizatorilor implicati in activitatile de flux, in vederea redistributiei controlate a sarcinilor si balansarii incarcarii intre utilizatori
q) Sistemul va oferi suport pentru monitorizarea respectarii/depasirii termenelor setate pe activitati. Sarcinile sau fluxurile depasite vor fi marcate vizual in interfata.
r) Posibilitatea de a configura sistemul astfel incat sa ia decizii automate prestabilite in cazul in care termenul limita al unei activitati din cadrul unui flux a fost depasit.
s) Posibilitatea de a configura sistemul, astfel incat un manager sa poata monitoriza sarcinile repartizate spre rezolvare angajatilor din subordine, pe intervale de timp. Un manager va trebui sa aiba acces rapid la un raport care sa contina toata documentele la care lucreaza subordonatii sai si informatii despre starea acestor documente. In cazul in care documentele sunt pe flux, raportul trebuie sa indice numele fluxului, activitatea/activitatile de pe flux si utilizatorul/utilizatorii la care se afla documentul in lucru. Managerul trebuie sa poata vizualiza documentul direct din raport. De asemenea, raportul trebuie sa poata fi filtrat dupa utilizatori subordonati, stari ale documentelor si perioada.

Managmentul termenelor de executie pe flux

Sistemul trebuie sa permita se poata defini termeni de executie atat pe fiecare activitate din cadrul unui flux electronic cat si pe o secventa de activitati dintr-un flux.

a) Un administrator trebuie sa poata seta termene de finalizare pentru fiecare activitate in parte
b) De asemenea, un administrator trebuie sa poata sa seteze activitatile in care executantul unui flux va putea suprascrie termenul de executie al unei secvente de activitati urmatoare. Astfel, administratorul va putea seta in orice punct al fluxului si de un numar nelimitat de ori urmatoarele aspecte:

- Activitatea sursa (locul de unde se va putea suprascrie termenul de executie);
- Rezolutia/Rezolutiile de finalizare a activitatii sursa (rezolutia care determina de cand se masoara termenul setat)
- Activitatea destinatie (activitatea la care se termina masurarea termenului setat in activitatea sursa);
- Rezolutia/Rezolutiile de finalizare a activitatii destinatare (rezolutia care determina finalizarea termenului setat)

c) Daca un user este intr-o activitate sursa pentru un set de termene pe lucrare, atunci el va avea optiunea sa seteze valori pentru termenele pe activitate.
d) Orice termen pe activitate setat de catre alti utilizatori va putea fi vizualizat de catre utilizatorul care efectueaza sarcina
e) Setarea de termene pe activitate este configurabila la nivel administrator dar optional la nivel de user. Astfel, daca un utilizator are posibilitatea de a seta termen intr-o activitate, dar nu face acest lucru, atunci termenul nu se mai aplica.
f) Toti utilizatorii vor putea vedea termene setate pe flux
g) Sistemul va trebui sa genereze automat notificari la apropierea termenului de executie precum si la depasirea acestuia

Monitorizarea activitatii subordonatilor

Sistemul trebuie sa permita ca utilizatorii cu pozitii de conducere si avand utilizatori in subordine sa poata vizualiza un raport cu documentele procesate de catre toti utilizatorii subordonati incepand cu prima zi a lunii anterioare.
Raportul trebuie sa furnizeze informatii privind: numele utilizatorului care a procesat documente de un anumit tip, numele documentului, starea curenta a acestuia (in biblioteca/ trimis pe flux/ in lucru colaborativ/ etc.), detalii privind locatia curenta a documentului si data ultimei implicari a utilizatorului pe acel document, cu lista tuturor implicarilor utilizatorului pe tooltip.

Fluxuri de lucru pe terminale mobile

a) Pentru utilizatori cu rol de decizie sistemul trebuie sa permita accesul la fluxurile electronice de documente de pe terminale mobile prin intermediul unei aplicatii dedicate. Utilizatorii trebuie sa poata interactiona cu sarcini primite pe telefonul mobil.
b) Functionalitatea trebuie sa fie disponibila pe mobil in permanenta si sa poata fi trecuta de utilizator in fundal.
c) Sistemul trebuie sa permita accesul de pe terminale mobile atat la sarcinile active, cat si sarcinile finalizate. Sarcinile noi trebuie sa fie evidentiate de restul sarcinilor active. Sarcinile depasite trebuie sa fie marcate suplimentar.
d) Pentru fiecare sarcina in parte sistemul trebuie sa permita:
    a. acces la informatii de detaliu despre sarcina primita: numele documentului, expeditorul, starea, nivelul de prioritate, activitatea de pe flux, data la care s-a emis sarcina si termenul de realizare;
    b. acces la documentele specifice sarcinii (documentul principal si atasamente), iar in cazul documentelor de tip formular afisarea pe terminal a campurilor si valorilor acestora;
    c. vizualizarea in ordine cronologica a rezolutiilor acordate anterior pe fluxul electronic;
    d. vizualizarea setului de rezolutii posibile de acordat si selectarea unei rezolutii pentru activitatea curenta de pe flux;
    e. redactarea unui comentariu pe flux, inainte de finalizarea sarcinii;
    f. vizualizarea destinatarilor posibili si selectiarea destinatarului/destinatarilo catre care se trimite documntul mai departe pe flux;
e) In cazul finalizarii fluxului, utilizatorul trebuie sa poata selecta pe terminalul mobil in ce folder din biblioteca electronica a sistemului se salveaza documentul.

6.7.7 Registratura electronica

Sistemul va pune la dispozitie un modul de tip registratura electronica cu urmatoarele functionalitati:

a) Numerotarea documentelor in regim automat, semi-automat sau manual, dupa o schema flexibila de numerotare

b) Asociarea fiecarui utilizator cate unui registru de documente personale pentru fiecare nivel de clasificare, care sa tina evidenta pe tuturor documentor adaugate in sistem de acel utilizator pe nivele de clasificare
c) Asocierea fiecarui utilizator a unui cate unui registru al documentelor electronice procesate pentru fiecare nivel de clasificare, care sa tina evidenta pe nivele de clasificare a tuturor documentor pe care un utilizator le-a primit prin intermediul fluxurilor electronice de lucru
d) Asociarea unui registru general pe fiecare structura din sistem, registru electronic in care vor fi inregistrate toate documente oficiale ale acelei structuri. Acest registru va tine evidenta documentelor intrare in structura, precum si evidenta documentelor care ies din structura sau sunt depuse in arhiva
e) Toate registrele trebuie inregistrate intr-un registru unic in care se tine evidenta tuturor registrelor folosite in sistem

Sistemul trebuie sa permita accesul la registrele electronice doar pe baza unor roluri specifice. Registrul general de intrari si iesiri trebuie sa indice starea la un moment dat a oricarui document din sistem. Accesul la documentele din registrul general de intrari si iesiri trebuie sa tina cont, suplimentar, de drepturile utilizatorilor pe categorii de documente si de nivelurile de clasificare.
Acordarea numerelor de inregistrare in registrul general intrari si iesiri se va face printr-un pas special de ingregistrare de pe fluxurile electronice de documente.

6.7.8 Mesagerie organizationala si notificari

Functionalitati solicitate:

a) Sarcinile de lucru in cadrul sistemului vor fi transmise sub forma de mesaje in interfata si vor fi vizualizate de fiecare utilizator in sub forma unui inbox virtual din spatiul de lucru propriu
b) Serviciul trebuie sa poata gestiona cu prioritate anumite sarcini de lucru, conditionat de evenimente specifice care marcheaza prioritatea
c) Utilizatorii trebuie sa poata fi notificati inainte de expirarea unei sarcini sau a intregii instante de flux (procent din timpul ramas, configurabil), precum si la expirarea timpului asociat unei sarcini de lucru primite sau al intregii instante de flux
d) Posibilitatea de a defini notificari la modificarea starii unui document pe flux si la adaugarea/retragerea acestuia din biblioteca.

6.7.9 Managementul sarcinilor (in afara fluxurilor de lucru)

Sistemul trebuie sa permita transmiterea unor sarcini sau cereri de lucru unor utilizatori, in afara fluxurilor electronice de documente. Aceste sarcini sau cereri de lucru vor avea un caracter formal si se vor monitoriza ca atare. Modulul trebuie sa permita urmatoarele functionalitati:

a) Sa se poata defini de catre administrator tipuri de sarcini sau cereri de lucru;
b) O sarcina sau o cerere de lucru sa poata fi adresata de catre un utilizator altui utilizator, fara sa respecte in mod necesar linia ierarhica din organigama;
c) Posibilitatea numirii unor supervizori pentru anumite sarcini sau cereri de lucru, care sa aiba vizibilitate in orice moment asupra stadiului de realizare a sarcinilor pe care le supervizeaza
d) Posibilitatea definirii unor termene limita de executie pentru sarcinile sau cererile de lucru;
e) Atat initiatorii sarcinilor cat si cei care rezolva sarcinile trebuie sa aiba posibilitatea de a atasa documente sarcinii
f) Posibilitatea de a realiza operatii privind sarcinile de lucru primite, emise, supervizate (vizualizare, adaugare, cautare) in functie de roluri specifice diferentiate. Sistemul trebuie sa permita monitorizarea sarcinilor primite, emise si supervizate si afisarea unor indicatori de stare si progres. Indicatorii de progres sa se evidentieze procentual si grafic. Raportul de monitorizare trebuie sa poata fi exportat intr-un fisier de tip xls. Starea asociata unei sarcini va putea avea urmatoarele valori: Deschisa, In lucru, Rezolvata, Redeschisa, Inchisa. La fiecare schimbarea a starii, sistemul va trimite mail-uri de notificare catre toti cei implicati in rezolvarea acelei sarcini.
g) Utilizatorul responsabil cu rezolvarea unei sarcini va putea acorda doar una din starile: In lucru sau Rezolvata, iar supervizorul va putea modifica starea sarcinii doar cu urmatoarele valori: Deschisa, Redeschisa, Inchisa;
h) Adaugarea de comentarii de tip text la fiecare schimbare a starii unei sarcini;
i) Cautare rapida si cautare avansata multicriteriala de sarcini;
j) Vizualizarea instoricului modificarilor efectuate asupra unei sarcini

k) Posibilitatea de a fi configurat astfel incat sa trimita automat si la intervale regulate de timp notificari pin email pentru raportarea stadiului de realizare a unei sarcini. De asemenea, sistemul trebuie sa ofere initiatorului posibilitatea de a selecta lista persoanelor care vor fi notificate.
l) Integrare cu Microsoft Outlook astfel incat sarcinile sa figureze in Calendar si in lista de task-uri, fiind accesibile astfel accesibile atat din clientul solid MS Outlook cat si de pe web (Outlook Web Acces) si de pe terminalele mobile care suporta suita MS Outlook.
m) Integrare cu echipamente mobile printr-o aplicatie dedicata, astfel incat utilizatorii sa poata vizualiza de pe terminale mobile sarcinile si starea lor si sa raporteze modificari de progres sau de stare.

6.7.10 Indicatori si rapoarte

Sistemul trebuie sa fie capabil sa genereze automat indicatori si rapoarte configurabile referitoare la:

a) Starea fluxurilor in lucru
b) Incarcarea utilizatorilor (general, specific, utilizatori in subordinea utilizatorului curent)
c) Fluxuri finalizate
d) Timpul mediu de executie pe flux
e) Timp mediu de executie per activitate per flux
f) Gradul de implicare al utilizatorilor per instanta per flux

Modulul trebuie sa permita realizarea de rapoarte:

a) pentru o perioada de timp selectata;
b) pentru o anumita diviziune organizatorica;
c) per fluxuri, per activitati;
d) rapoarte agregate;

Accesul la modulul de raportare trebuie sa fie disponibil doar utilizatorilor cu drepturi de acces specifice.

6.7.11 Administrare

Administrarea drepturilor

Functionalitati solicitate:

a) Sistemul trebuie sa permita cotrolul accesului la functionalitati si date va fi gestionat printr-o schema de drepturi multi-nivel, schema ce va fi verificata la fiecare operatie atat in mod preventiv cat si reactiv
b) Interfata grafica trebuie sa fie dinamica, in sensul ascunderii integrale a datelor si functionalitatilor la care un utilizator nu are acces
c) Executia unei operatii sau de acces la date va fi verificata in mod preemtiv in raport cu drepturile utilizatorului de a accesa acele date
d) Drepturile de acces vor fi implementate prin intermediul unei scheme ierarhice si dinamice de roluri. Astfel, unui rol i se vor putea asocia drepturi de acces pe diferite nivele (tip document atribute ale documentelor, gradul de clasificare, instanta de document)
e) La nivelul fluxurilor de documente, sistemul trebuie sa permita acordarea de drepturi pe setul de fluxuri disponibile pentru fiecare utilizator. De asemenea, la nivelul fiecarei activitati din flux, trebuie sa existe posibilitatea de a da drepturi referitor la cine sunt utilizatorii care pot efectua acea activitate si care sunt drepturile acestora in cadrul respectivei activitati
f) La nivelul bibliotecii, sistemul trebuie sa permita acordarea granulata a drepturilor de acces la nivel de sectiuni/subsectiuni din biblioteca, cat si la nivelul setului de operatii disponibile (vizualizare, modificare, preluare, retragere)
g) Sistemul trebuie sa permita gestiunea documentelor clasificate, in sensul de a suporta acordarea, in mod obligatoriu, a unui grad de clasificare pentru fiecare document introdus in sistem conform standardelor nationale de protectie a informatiilor clasificate in Romania (HG 585/2002). De asemenea, orice utilizator va avea asociat un nivel maxim de acces la documente clasificate, nivel ce va reglementa, in orice conditii, setul de documente la care un utilizator are acces.

Administrarea utilizatorilor

Functionalitati solicitate:

a) Adaugare, modificare, inactivare, stergere utilizatori si date asociate

b) Asocierea de date personale (nume, prenume, titlu, functie, locatie, cod de identificare, adresa e-mail, etc)
c) Asociarea de roluri simple sau compuse si posibilitatea de a delega aceste roluri fie de catre utilizator, fie de catre administrator catre un alt utilizator pe o perioada data. Delegarea rolurilor presupune ca toate drepturile asociate rolurilor delegate sunt preluate automat si temporar de utilizatorul catre care se deleaga. La nivelul fluxurilor electronice de documente, utilizatorul delegat va prelua atat sarcinile curente al utilizatorului cat si cele care ii vor reveni utilizatorului initial pe perioada delegarii
d) Sistemul trebuie sa permita preluarea utilizatorilor si a drepturilor acestora dintr-un structura de tip LDAP sau Active Directory
e) Personalizarea interfetei in functie de rolurile si drepturile asociate utilizatorului sau grupului de utilizatori

Administrarea structurii organizatorice

Sistemul trebuie sa permita definirea si mentenanta unor strucuri organizatorice multiple, de tip ierarhic. Astfel sistemul trebuie sa permita definirea unui numar nelimitat de structuri organizatorice asociate intre ele sau independente, si pentru fiecare structura, sistemul trebuie sa permita urmatoarele:

a) Definirea de structuri si substructuri, iar pentru fiecare structura sa se poata defini numele, tipul, un cod de identificare, pozitia in ierarhie
b) Definirea de persoane in ierahie cu precizarea functiei, pozitiei in structura (sef, subaltern, etc)
c) Modificarea facila a structurii de catre administrator (adaugarea, stergerea sau mutarea entitatilor sau utilizatorilor din structura)
d) Pastrarea istoricului modificarilor din cadrul unei structuri sau diviziune de structura
e) Adaugare/modificare/stergere/cautare drepturi de acces pe care le poate avea un rol pentru o ierarhie (vizualizare, printare, editare, stergere)
f) Suport pentru definirea de nomenclatoare asociate structurii organizatorice (pozitii, adrese, etc)
g) Suport pentru vizualizarea grafica a structurilor organizatorice definite in sistem
h) Exportul organigramelor structurilor organizatorice definite in sistem in fisiere de tip imagine

Structurile organizatorice vor fi utilizate pentru a face rutarea automata a sarcinilor din fluxurile electronice de lucru, pe cale ierarhica ascendenta sau descendenta.

6.7.12 Auditarea

Sistemul trebuie sa implementeze un modul dedicat de audit si jurnalizare a tuturor operatiilor efectuate in sistem, cu evidentierea autorului, datei si orei, adresei de IP si descrierea operatiei.
In cazul operatiilor asupra documentelor se doreste si evidentierea nivelului de clasificare al documentului.
Accesul la modulul de audit se va face doar pe baza unor roluri specifice de administrare loguri. Rolurile de administrare a logurilor trebuie sa poata fi definite si acordate cat mai granulat, pe categorii de operatii. Modulul trebuie sa permita cautare multicriteriala a inregistrarilor din jurnalul de audit, urmatoarele criterii de cautare fiind disponibile: autor, data si ora, adresa de IP, categoria de operatie, descrierea operatiei, nivelul de clasificare al documentului si nivelul de clasificare al utilizatorului la momentul operatiei.
De asemenea, modulul trebuie sa permita exportul rapoartelor de audit in .xls, .pdf sau .html, iar la generarea exportului sistemul va cere utilizatorului semnarea raportului de audit, in vederea asigurarii integritatii informatiei si verificarii ulterioare. In cazul exportului raportului in format .pdf, semnarea raportului trebuie sa respecte standardul PAdES standard.Modulul trebuie sa permita si adaugarea rapoartelor direct in aplicatie.

Submodul dedicat pentru audit de securitate consolidat

Sistemul trebuie sa furnizeze si un submodul de audit consolidat, dedicat monitorizarii si corelarii informatiilor legate de utilizarea subsistemelor IT furnizate si accesul la aceste subsisteme. In acest sens, modulul va trebui sa furnizeze urmatoarele functionalitati:

a) Integrarea modulului cu celelalte subsisteme IT oferite sau existente pentru preluarea de loguri specifice fiecarui subsistem. Logurile trebuie transmise in format XML semnat si criptat si trebuie sa contina informatii standard precum: identificator subsistem IT, tip operatie, utilizatorul care a efectuat operatia, data executiei, obiectul operatiei, descriere a evenimentului.
b) Investigarea si analiza secventelor complete de acces prin sub-sisteme si analiza operatiunilor efectuate de utilizatori in subsistemele IT monitorizate. Se vor genera reprezentari grafice explicite care sa evidentieze cronologia evenimentelor si sa permita analiza in adancime (tehnica de tip zoom-in, zoom-out) a unor astfel de cronologii.

c) Analiza secventelor complete de acces pentru descoperirea de pattern-uri de activitati ale utilizatorilor diferentiate pe tip de utilizator, tip de operatii etc.
d) Integrarea cu sistemul de gestiune a smartcard-urilor/token-urilor pentru preluarea informatiilor detaliate legate de identitatea si credentialele utilizatorilor.
e) Punererea la dispozitie a unor API-uri care sa permita conectarea altor aplicatii generatoare de loguri de securitate.

Submodul dedicat pentru detectia in timp real a comportament suspect

Acest submodul va permite analiza in timp real al comportamentului unui utilizator in raport cu o cu subsistemele IT securizate la care acesta are acces. Modulul va semnala orice abateri de la un anumit sablon impus si va genera alarme si notificari si va fi capabil sa trimita un set de comenzi sistemelor de securitate asociate. In acest sens, modulul va trebui sa furnizeze urmatoarele functionalitati:

a) definirea de sabloane de secvente de evenimente permise care sa includa evenimente primite de la senzori, evenimente legate de operarea subsistemelor IT monitorizate. Sabloanele trebuie sa permita atat definirea succesiunii cronologice de evenimente, configurarea evenimentelor permise (tip de eveniment, set de sub-operatii permise, locatie, rol asociat, perioada de valabilitate etc.) dar si definirea regulilor de tranzitie de la un eveniment la altul (succesiune stricta, variante alternative, timp maxim permis intre evenimente etc.)
b) incarcarea acestor sabloane de secvente in sistem precum si modificarea celor existente in orice moment de timp, fara necesitatea repornirii modulului
c) monitorizarea tuturor logurilor inregistrate si analiza in timp real a logurilor provenite de la subsistemele IT monitorizate, pentru detectia unor comportamente diferite de cele predefinite
d) Alertarea in caz de abateri de la comportamentul predefinite, prin trimiterea de notificari pe canale multiple (notificari in sistem, e-mail) catre administratorii de securitate responsabili, in functie de responsabilitatea si disponibilitatea acestora (locatie, rol, timp de raspuns etc.)
e) Integrarea modulului cu sistemul de securitate fizica catre care sa poata sa trimita un set de comenzi
f) Generarea de statistici si rapoarte referitoare la tipurile de abateri, frecventa lor, tipurile de utilizatori implicati etc.

6.7.13 Submodul dedicat clasificarii de documente si mesagerie

Acest modul trebuie sa permita utilizatorilor sa stabileasca grade de clasificare pentru documentele emise sau pentru mailurile pe care le trimit, sa permita verificarea fluxurilor de informatii sensibile si sa se poata integra cu o solutie de Data Lost Prevention (DLP).
Pentru fiecare document creat cu suita MS Office, respectiv pentru fiecare email trimis utilizatorul trebuie sa poata acorda un grad de clasificare si sa poata stabili un topic (categorie de interes). La trimiterea documentului prin email trebuie sa se poata valida trimiterea, pentru protejarea informatiei cu caracter sensibil.
Utilizatorul va clasifica obligatoriu un document sau un email, folosind grade de clasificare predefinite. Modulul nu va permite salvarea documentului daca nu a fost ales un grad de clasificare pentru document, iar in cazul in care utilizatorul nu a stabilit gradul de clasificare al documentului, acesta va fi cerut la salvare intr-o fereastra de tip pop-up. Unui document existent nu i se va putea schimba gradul de clasificare decat cu unul mai restrictiv.
Submodulul trebuie sa permita configurarea din interfata de administrare ca la trimiterea prin email a unui document clasificat ca si confidential sau secret, utilizatorului sa i se solicite semnarea documentului cu certificat digital.
Submodulul trebuie sa permita definirea unor constrangeri pe anumite cuvinte cheie si grade de clasificare, iar la salvarea documentului va trebui sa se verifice concordanta dintre constrangeri si gradul de clasificare definit de utilizator. In cazul detectarii unei neconcordante intre gradul de clasificare si restrictiile de clasificare, se va afisa un mesaj de eroare corespunzator.
In cazul emailului modulul va trebui sa permita validarea concordantei intre gradul de clasificare al emailului si gradul de clasificare al documentului din atasament. Gradul de clasificare al unui mesaj poate fi modificat doar de catre persoana care a initiat mesajul. De asemenea, si in cazul mesajelor existente nu va fi posibila schimbarea gradului de clasificare decat cu unul mai restrictiv.

6.7.14 Arhivare

Modulul de arhivare trebuie sa functioneze ca un serviciu suport ce permite arhivarea tuturor documentelor vechi, care nu mai sunt accesate frecvent, corelat cu termenele stabilite prin lege si posibilitatea de acces la acestea pe baza de cerere. Astfel, functionalitatile de arhivare electronica trebuie sa respecte cerintele legii 135/2007 privind arhivarea documentelor in forma electronica.

Functionalitati solicitate:

a) Sa permita stocarea datelor pe trei nivele:
   1. online (in baza de date)
   2. nearline (suport accesibil direct din aplicatie)
   3. offline (pe medii interne si externe magnetice sau optice)
b) Sistemul trebuie sa ofere facilitati de auto-arhivare.
c) Sistemul trebuie sa permita definirea perioadei de pastrare pentru fiecare categorie de documente in parte.
d) Sistemul trebuie sa restrictioneze posibilitatile de modificare a documentelor electronice care au fost arhivate.
e) Sistemul nu trebuie sa permita mutarea in arhiva electronica a unor documente aflate pe fluxuri electronice de documente sau in colectile personale de documente ale utilizatorilor.
f) Sistemul trebuie sa permita definirea politicilor de arhivare pe baza unui set extins de criterii de arhivare (tip document, vechime document, structura organizatorica, grad de clasificare etc.). Aceste politici vor folosi la trecerea documentelor din online in nearline. Sistemul va face selectia documentelor candidate pentru arhivare electronica si trecerea lor in arhiva in baza politicilor de arhivare, definite in sistem de catre administratorul arhivei electronice.
g) Sistemul trebuie sa permita un set extins de operatii asupra politicilor de arhivare (adaugare, vizualizare, modificare, activare, dezactivare, stergere). Stergerea politicilor sa fie posibila doar in cazul in care nu are atasate sesiuni de arhivare.
h) Politicile de arhivare trebuie sa poata fi setate sa ruleze manual, la initiativa administratorului, sau automat.
i) Documentele trebuie sa fie trecute din online in nearline doar in baza unor politici definite pentru categoria din care fac parte. Daca pentru un tip de document nu se defineste niciodata o politica de arhivare, sistemul va pastra permanent documentele corespunzatoare acelui tip de document.
j) Documentele trebuie sa fie trecute din nearline in offline pe baza vechimii acestora in spatiul de arhiva nearline, vechime care va putea fi setata de catre administratorul arhivei cu ajutorul unui parametru de sistem.
k) La depunerea documentelor in arhiva electronica sistemul trebuie sa solicite semnarea digitala a documentelor de catre titularul dreptului de dispozitie asupra documentelor, pentru a garanta integritatea ulterioara a documentelor in arhiva. Semnarea se va face cu un certificat calificat.
l) La depunerea documentelor in arhiva electronica sistemul sa asigure semnarea digitala de catre administratorul arhivei, pentru a garanta integritatea ulterioara a documentelor pastrate in arhiva. Semnarea se va face cu un certificat calificat in mod automat pentru tot setul de documente asociat politicii de arhivare.
m) La depunerea in arhiva electronica fiecarui document electronic trebuie sa i se asocieze o fisa electronica de date, care sa contina atribute ale documentului.
n) Documentele electronice arhivate si fisele electronice asociate trebuie referite intr-un registru electronic de arhivare, unic la nivelul unei structuri organizatorice.
o) Fisa electronica de date trebuie sa poata fi accesata prin intermediul registrului electronic de arhivare, indiferent daca documentul se afla in nearline sau offline.
p) Pentru consultarea documentelor arhivate electronic sistemul trebuie sa permita cautarea dupa un set extins de criterii de cautare si in baza unui drept special de cautare in arhiva. Cautarea trebuie sa se realizeze intre referintele din registrul de arhivare electronica.
q) Regasirea documentelor in arhiva electronica trebuie sa tina cont de drepturile utilizatorilor asupra categoriilor de documente, respectiv de nivelurile de clasificare ale documentelor si ale utilizatorilor.
r) Daca documentele sunt in arhiva nearline, cautarea in registrul de arhivare electronica trebuie sa aiba ca rezultat un set de atribute referitoare la document si acces la fisa electronica, respectiv la document.
s) Daca documentele sunt in arhiva offline, cautarea in registrul de arhivare electronica trebuie sa aiba ca rezultat un set de atribute referitoare la document si acces la fisa electronica. Pentru consultarea documentului din offline sistemul trebuie sa permita lansarea unor cereri de reactivare a documentelor.
t) Sa permita reactivarea documentelor arhivate in scopul vizualizarii, in mod parametrizabil. Reactivarea documentelor electronice se va face pentru o perioada limitata de timp, perioada configurabila din interfata de administrare.
u) Aplicatia de arhivare sa permita criptarea/decriptarea automata folosind certificate digitale.

v) La consultarea documentelor din arhiva electronica sistemul trebuie sa verifice valabilitatea semnaturii electronice a titularului dreptului de dispozitie asupra documentului (validitatea certificatului calificat).

6.8 Platforma pentru instruirea utilizatorilor si lucru colaborativ

Platforma pentru instruire si lucru colaborativ va fi utilizată pentru utilizatorii sistemului in vederea obtinerii celor mai bune rezultate privind utilizarea noilor servicii electronice intr-un mod cat mai rapid la costuri minime.
Instruirea urmărește o pregătire continuă a utilzatorilor astfel încât acestia sa poata utiliza la maxim benificiile noului sistem.

6.8.1 Caracteristici tehnice ale platformei de instruire on-line

Platforma de instruire va trebui sa aiba următoarele capabilități:

- Sa functioneze pe tehnologie cloud Microsoft Azure
- Sa permita instruirea utilizând instrumente moderne de predare cum ar fi ecrane touch, table interactive cu rolul de ”tabla clasei”
- Sa permita instruirea participanților în aceeași locație cu instructorul (aceeași încăpere)
- Sa faca posibilă instruirea participanților atunci când aceștia nu se află în aceeași încăpere cu instructorul. Participantii pot fi:

În alte încăperi aflată în altă locație

În fața computerului personal conectați la internet

O parte în aceeași încăpere cu instructorul, o parte în fața computerelor personale, o parte în alte încăperi (fără prezența fizică a instructorului)

- Instruirea participanților sa fie posibilă în mod similar indiferent de locul unde aceștia sunt prezenți în sensul că:

Toți pot interacționa cu instructorul (pe care în văd și îl aud)

Toți pot interacționa unii cu alții (se pot auzi și vedea)

”Tabla clasei”, ca instrument de instruire poate fi utilizată în mod comun (toți văd același conținut și pot interacționa cu acest conținut)

  - Instruirea sa fie condusa de un instructor certificat de autoritatea care pune la dispozitie platforma.

- Platforma sa poata permite prin intermediul ”tablei clasei”:

Scrierea, desenarea

Partajarea (utilizarea în comun) de filme, animații, imagini

Transmiterea de imagini a unor obiecte fizice pe care instructorul dorește să le utilizeze (documente, obiecte specifice instruirii de urgență cum ar fi: extinctoare, măști de oxigen, în general echipament specific de intervenție)

- Platforma sa permita autoinstruire prin parcurgerea cursurilor predate anterior. Aceste cursuri sa poata fi parcurse de utilizatori fără a fi necesară prezența unui instructor.
- Platforma sa permita examinarea cunoștințelor acumulate de participanți prin:

Teste în scris

Teste orale

Testele efectuate indiferent de locul unde se află cei testați

- Platforma sa fie ușor de utilizat și sa necesite o curbă de învățare foarte mică. Astfel instrumentele ce se vor pune la dispoziție trebuie să fie similare cu cele din lumea reală și nu cu cele specifice IT. În acest sens, platforma:

Sa poata fi operata cunoscand noțiuni cum ar fi tablă, cretă, burete virtuale care sa se utilizeze similar ca cele din lumea reală

Sa aiba o intruziune minimă în activitatea de instruire – nu se solicită instructorilor și participanților să facă operațiuni tehnice complicate sau care să interfereze cu activitatea de predare cum ar fi vorbitul la microfon, comutare de imagini, comutare de sunet

- Platforma sa poata genera salvari ale cursurilor atat in format PDF cat si intr-un format propriu care sa poata fi apoi revizuit de cursanti ca un film.
- Participantii la curs sa poata intra intr-o sesiune de training oricand, avand instantaneu acces la cursul deja predat pana la momentul accesarii lui de catre participant. Accesarea unei sesiuni deja initiate sa se faca cu un cod PIN care este generat initiatorului cursului si care ulterior va fi furnizat tuturor cursantilor.

6.8.2 Functionalitati

”Tabla clasei” va fi o aplicație din cadrul platformei optimizată pentru dispozitive touch (table, tablete, ecrane, telefoane etc) care va fi utilizată intensiv în cadrul sesiunilor de instruire fie că participanții sunt în aceeași încăpere cu instructorul fie că o parte dintre aceștia se află la distanță.
Funcționalitățile pe care această aplicație trebuie să le ofere celor care o utilizează:

- **Scrierea**

Pe tablă sa se poata scrie utilizând un instrument tip ”pen” sau utilizând un obiect oarecare (chiar și degetul). Scrierea sa se faca ca în modul clasic, prin atingerea suprafeței.
Pentru situația în care sunt implicați participanți din alte locații, scrierea se va transmite către aceștia pe măsură ce se produce. Aceștia trebuie sa vada pe dispozitivul propriu (altă tablă interactivă sau ecranul PC-ului propriu sau al tabletei etc.) scrierea celorlalți ca și când aceștia ar scrie chiar pe dispozitivul lor – în mod continuu.
Oricare dintre participanți sa poata utiliza dispozitivul propriu pentru a scrie pe ”tabla clasei” chiar și în paralel cu ceilalți. Scrisul trebuie sa se transmita către toți în aceeași manieră continuă și firească ca mai sus.

- **Ștergerea**

Pe tablă sa se poata șterge similar ca pe o tablă clasică. În acest sens sa fie utilizat un burete virtual – efectul de ștergere trebuie sa fie cât mai asemănător cu cel clasic.
Participanții la o sesiune de instruire care vor avea acces la ”tabla clasei” prin dispozitive touch proprii vor vedea ștergerea ca și când ar fi făcută pe dispozitivul lor. Mai mult, aceștia trebuie sa poata șterge chiar în paralel cu alți participanți sau cu instructorul.

- **Desenarea**

La tablă sa se poata desena similar cu desenarea pe o tablă clasică (prin atingere). Aplicația trebuie sa transmita desenarea similar cu scrierea și ștergerea către toți participanții.
Aceștia sa poata desena în același timp, acțiunea fiecăruia fiind vizibilă, în mod continuu tuturor.

- **Schimbare instrumente de scris , de ștergere, a fundalului**

Aplicația sa poata permite alegerea instrumentului virtual de scris (exemplu creta, pix, pensulă) precum și culoarea, grosimea sau tipul liniei produs de instrument.
Fundalul tablei trebuie sa fie customizabil – sa se poata modifica textura și culoarea.

- **Paginarea**

În timpul unei sesiuni de instruire sa se poata crea ”pagini” noi. De asemenea sa se poata naviga la paginile anterioare sau oricare pagină, sa se poata modifica ordinea paginilor, sa se poata șterge pagini sau conținutul unei pagini.
Trebuie sa existe o pagină specială al cărei conținut sa poata fi afișat rapid și oricând – acesta sa poata fi utilizată de exemplu pentru scrierea structurii cursului sau pentru orice alt scop care implică necesitatea de a reveni la acel conținut în mod repetat de-a lungul sesiunii de instruire. Pozitionarea acesteia trebuie sa fie intr-un mod neintruziv, usor de accesat.

- **Înregistrarea și redarea cursului**

Sesiunea de predare (tot ceea ce se întâmplă pe tablă) trebuie sa poata fi înregistrată în mod propriu marcata temporal sub forma de video când sunt participanți la distanță.
Obiectivul înregistrării este de a permite ulterior:

- vizionarea cursului în scop didactic de către voluntari care nu au participat live la curs
- reutilizarea cursului de către instructor cu posibilitatea de a-l modifica și de a crea un nou curs

- **Undo și redo**

Aplicația va trebui sa permita functii de undo și redo (anularea sau revenirea asupra unei comenzi și efectului acesteia) în numar de 10.

Functiile de undo și redo vor fi specifice unui dispozitiv în sensul că vor afecta numai comenzile efectuate de pe acel dispozitiv. Astfel un utilizator sa poata face undo sau redo numai comenzilor proprii în cazul în care acel utilizator folosește un dispozitiv touch propriu.
Instructorul sa poata face undo și redo numai comenzilor date către dispozitivul utilizat de acesta (exemplu tablă inteligentă touch)

- **Recunoaștere scris**

Aplicația va trebui sa recunoasca scrisul de mână. Efectul recunoașterii este vizibil către toți participanții indiferent cine îl inițiază.

- **Căutare online**

Aplicația va trebui sa permita căutari online pornind de la scrisul recunoscut prin functiile programate in aplicatie.
Căutarea pe internet se va face folosind motorul Google sau altul precum și folosind motoare specifice unei materii cum ar fi Wolfram Alpha pentru matematică sau Wikipedia.
Căutarea sa poata fi executată și direct prin introducerea de text de la o tastatură virtuală.
Efectul căutării sa fie vizibile către toți participanții indiferent cine îl inițiază. Mai mult, oricare dintre participanți sa poata continua căutarea sau navigarea pe internet – ceilalți sa vada în mod continuu efectul acțiunilor acestuia.

- **Play multimedia**

Aplicația sa permita redarea de conținut multimedia care este afișat tuturor perticipanților. Controlul privind: play, pauză, stop, înapoi, înainte este disponibil oricărui participant. Formatul multimedia sa fie jpg pentru poze si mp4 pentru video.

- **Partajarea informatiei de pe device-ul propriu**

Aplicația va trebui sa ofere posibilitatea utilizatorilor sa aduca sub forma de poze orice continut deja disponibil pe device-ul propriu. Pentru a aduce informatii de pe device-ul propriu aplicatia trebuie sa permita accesul la sistemul calculatorului fara a intrerupe cursul.

- **Spatiu de stocare propriu**

In aplicatie, fiecare utilizator va trebui sa aiba un spatiu de stocare propriu care va trebui sa stea pe cloudul Microsoft Azure. In acest spatiu, utilizatorii sa poata urca materiale multimedia cum ar fi poze in format jpg sau filme in format mp4.

6.8.3 Examinarea

Platforma de instruire trebuie să permită examinarea voluntarilor atât în aceeași sală de clasă cât și de la distanță.
Examinarea implică crearea testelor:

- crearea de teste clasice
- crearea de teste grilă
- crearea de teste orale, interactive

Examinarea implică planificarea testelor și a participanților la teste.
Examinarea implică desfășurarea testelor:

- clasice, în care participanții scriu și argumentează răspunsurilor
- grilă, în care participanții aleg răspasurile corecte
- orale, în care participanții răspund oral și utilizând ”tabla clasei” fie că sunt în aceeași încăpere cu examinatorul fie că sunt la distanță. Testele orale pot fi înregistrate similar sesiunii de predare pentru a fi evaluate ulterior.

Examinarea implică corectarea testelor și stocarea rezultatelor în dosarul voluntarului.
Corectarea testelor va fi făcută de examinator.

6.8.4 Autoinstruire

Platforma de instruire va permite utilizarea instrumentelor puse la dispoziție de aplicația ”tabla clasei” pentru a fi create cursuri destinate autoinstruirii.
În acest sens se solicită furnizarea a unui curs de prim ajutor creat cu aceste instrumente care va fi inclus în platforma livrată.
Cursurile pentru autoinstruire vor fi accesibile prin portalul informatic și pot fi parcurse utilizând o platforma „tabla clasei” pentru redarea acestora.

6.8.5 Infrastructura asociata

In cadrul proiectului furnizorul va asigura echiparea unei locatii pentru facilitatea de instruire a utilizatorilor. Aceasta va fi echipata minimal cu sistem de videoconferinta, tabla interactiva multitouch, videoproiector, dispozitive USB pentru cursanti, aplicatii specifice. Aceasta locatie va fi folosita de catre specialistii ce vor sustine cursurile. O alta locatie va fi folosita de catre cursanti in cadrul sesiunilor interactive.
Caracteristicile minimale ale tablei interactive ofertate vor fi:

- Diagonala minim 80 inch
- Input: senzor de imagine cu infrarosu
- Interfata de conectare: USB 1.1/2.0
- Rezolutie: 0.05 mm
- Acuratete: +/- 1,5 mm

Sistemul de video conferinta ofertat trebuie sa suporte definitie inalte HD 1080p, minim 3 locatii simultan, mod dinamic de afisare in dependenta cu numarul de participanti, posibilitate de transmitere prezentari in timpul transmisiei, sa suporte protocoale de VoIP tip H323, SIP, sa permita conectarea simultana a doua camere 720p/60fps, sa permita microfon cu functii de reducere zgomot si sa fie dotat cu minim 2 interfete LAN 100/1000 Mbps.

6.9 Infrastructura de chei publice

Este necesara implementarea unei infrastructuri cu chei publice pentru a raspunde la cerintele de integritate, autenticitate, confidentialitate si non-repudiere. Implementarea infrastructurii cu chei publice va avea in vedere urmatoarele cerinte:
Implementarea unei autoritati de certificare;

Materialul criptografic al utilizatorilor va fi stocat pe token USB (generare, utilizare chei criptografice);

Crearea unui sablon de politica de certificare.

Infrastructura cu chei publice va include toate serviciile aferente unei astfel de solutii:

Serviciul de gestiune a certificatelor digitale;

Modul de recuperare a cheilor private de criptare;

Serviciul de validare online a starii certificatului;

Serviciul de marcare temporala;

Pentru validarea on-line a starii certificatului si pentru marcarea temporala se va furniza o solutie de management centralizat al cheilor criptografice utilizand dispozitive hardware criptografice certificate FIPS 140-2 Level 3.
Pentru managementul infrastructurii de chei publice se va folosi si propune o statie de lucru dedicata, care sa poata gestiona in conditii de securitate informatia vehiculata.
Componentele solutiei de infrastructura vor fi protejate prin echipamente dedicate de tip firewall. Echipamentele pentru infrastuctura de chei publice vor fi insalate in camera tehnica unde sunt instalate in prezent si echipamentele autoritatii de certificare existente.

6.9.1 Gestiunea certificatelor digitale

Serviciul de gestiune a certificatelor digitale va fi responsabil cu administrarea cheilor si certificatelor utilizatorilor pe toata durata acestora de viata. Aceasta impune urmatoarele operatii:
Generarea cheilor private ale autoritatii de certificare radacina

Generarea certificatelor autoritatii de certificare radacina

Generarea cheilor si cererilor de certificare ale autoritatilor subordonate

Instalarea certificatelor autoritatilor de certificare subordonate

Generarea cererilor de certificat pentru certificare incrucisata

Generarea cheilor certificatelor utilizatorilor

Inregistrarea cererilor de certificat ale utilizatorilor, inclusiv provenind de pe dispozitive mobile

Emiterea certificatelor utilizatorilor, inclusiv pe dispozitive mobile

Revocarea certificatelor utilizatorilor

Reinnoirea certificatelor utilizatorilor

Recuperarea cheilor private de criptare.

Publicarea certificatelor si CRL-urilor autoritatilor de certificare in serviciul de directoare LDAP v3

Publicarea certificatelor utilizatorilor in serviciul de directoare LDAP v3

Pentru certificatele emise de RootCA se va putea utiliza un sistem software-hardware off-line neconectat la retea. Acest serviciu va fi implementat de autoritatea de certificare. Pentru a exista un nivel de incredere maxim in certificatele gestionate de aceasta autoritate, aceasta trebuie sa permita o arhitectura bazata pe doua zone de securitate ce pot fi separate atat logic cat si fizic. Zonele vor delimita clar inregistrarea utilizatorilor de administrarea certificatelor si a cheilor.
Pentru a obtine un nivel de securitate ridicat este necesar ca zonele publica si privata ale autoritatii de certificare sa nu fie conectate prin intermediul echipamentelor de retea. Astfel se poate proteja zona privata in cazul in care zona publica a fost compromisa. Pentru functionarea solutiei este nevoie insa de transfer de date intre cele doua zone, si pentru aceasta se vor utiliza echipamente non-ethernet de transfer si filtrare a informatiilor.

Acest echipament trebuie sa permita doar transferul de date dintr-o zona in alta, nepermitand executia de comenzi sau aplicatii intre cele doua zone. De asemenea dispozitivul trebuie sa se blocheze in cazul in care datele transferate nu sunt codificate ASCII. Deblocarea dispozitivului dupa o tentativa de transfer de informatii nepermise se va face doar manual.
In zona de inregistrare a utilizatorilor vor fi plasate serviciile cu caracter public a autoritatii de certificare:
publicarea certificatelor si CRL-urilor autoritatilor

publicarea certificatelor utilizatorilor

componentele de inregistrare automata a cererilor de certificate pentru dispozitive de retea

In zona de administrare a certificatelor si cheilor vor fi plasate serviciile cu caracter sensibil:
Generarea cheilor private ale autoritatii de certificare radacina

Generarea certificatelor autoritatii de certificare radacina

Generarea cheilor si cererilor de certificare ale autoritatilor subordonate

Instalarea certificatelor autoritatilor de certificare subordonate

generarea cheilor criptografice de criptare;

semnarea CRL-urilor autoritatilor;

emiterea certificatelor utilizatorilor;

administrarea tipurilor de certificate

administrarea politicilor de utilizare a certificatelor

administrarea operatorilor autoritatii de certificare.

Cheile si certificatele utilizatorilor (persoane sau dispozitive) vor putea fi gestionate atat in format software cat si pe dispozitive criptografice de tip smartcard/tokenUSB. Pentru dispozitivele criptografice este necesar ca acestea sa fie conforme cu standardul FIPS 140-2 level2.
Autoritatea de certificare va utiliza dispozitive criptografice hardware ce indeplinesc standardul FIPS 140-2 level 3 (minim 500 operatiuni RSA 1024/sec) pentru toate operatiunile ce implica utilizarea cheilor private (semnare de certificate, de CRL-uri, recuperare chei)
Pentru operarea autoritatii de certificare este necesar un nivel de securitate crescut atat pentru autentificare cat si pentru protejarea informatiilor ce vor fi transmise. Pentru aceasta este necesara implementarea unei metode de autentificare ce permite criptarea datelor transmise si identificarea sigura a celor doua entitati ce comunica. In acest scop se va folosi protocolul SSL utilizand dubla autentificare.
Autoritatea de certificare va fi implementata utilizand o arhitectura in care autoritatea de certificare radacina va fi utilizata doar in caz de necesitate, putand fi pastrata offline. Operatorii autoritatii de certificare radacina vor fi diferiti de operatorii autoritatii de certificare.
Certificatele ce vor permite operarea autoritatii de certificare si certificatele utilizatorului nu vor fi semnate utilizand aceleasi chei criptografice. Pentru a indeplini aceasta cerinta este necesara implementarea unei infrastructuri PKI complet separata pentru gestiunea certificatelor operatorilor si a sistemelor din infrastructura PKI. Aceasta va implementa obligatoriu urmatoarele cerinte:
autentificare cu certificat digital;

sistemul de autorizare va fi unul bazat pe roluri;

infrastructura va genera certificate digitale pentru sistemele autoritatii de certificare accesate de operatori;

ierarhia pe care vor fi emise certificatele operatorilor va fi separata complet de ierarhia in care vor fi generate certificatele utilizatorilor (autoritate radacina separata)

cheile autoritatii de certificare vor fi pastrate pe dispozitive criptografice hardware.

Cheile operatorilor sistemului vor fi generate obligatoriu pe dispozitive criptografice de tip smartcard, certificate FIPS 140-2 level 2.
Pentru a putea fi utilizata de cat mai multe servicii, autoritatea de certificare trebuie sa permita stocarea certificatelor autoritatilor,a listelor de certificate revocate si a certificatelor utilizatorilor intr-un serviciu de directoare LDAP v3/X.500 accesibil utilizatorilor fara a fi necesara autentificarea la acesta.
Solutia trebuie sa permita emiterea tuturor tipurilor de certificate prin implementarea extensiilor de certificate conform standardului X.509 v3. De asemenea, se vor putea implementa extensii private, specifice aplicatiilor interne ale beneficiarului.
Solutia trebuie sa ofere functionalitati prin intermediul carora anumite operatiuni vor fi automatizate:
actualizarea CRL-ului autoritatilor de certificare subordonate

publicarea certificatelor si a CRL-urilor autoritatilor pe serverul LDAP v3

publicarea certificatelor si a CRL-urilor autoritatilor pentru a fi accesibile prin HTTP

publicarea certificatelor emise pe server LDAP v3

stergerea certificatelor revocate si expirate de pe serverul LDAP v3

notificarea administratorilor asupra iminentei expirarii certificatelor

Notificarile se vor face utilizand comunicatia prin mecanisme de tip e-mail.
Solutia implementata trebuie sa ofere mecanisme de monitorizare ale aplicatiilor si sistemelor componente:
monitorizarea functionarii serviciului de directoare LDAP v3

monitorizarea serviciului de publicare a certificatelor si CRL-urilor pe LDAP

monitorizarea starilor certificatelor si crl-urilor autoritatilor

Pentru indeplinirea cerintelor de inalta disponibilitate solutia trebuie sa permita instalarea serviciului intr-o arhitectura ce suporta failover.

Interfata va fi si in limba romana. In acest sens se vor prezenta capturi de ecran ale aplicatiei si manuale de utilizare.
Ofertantul va prezenta angajamentul de la producatorul aplicatiei prin care acesta garanteaza ca asigura functionalitatile cerute prin caietul de sarcini.
Se va avea in vedere certificarea nationala ca produs de securitate la nivel minim **Secret** de catre ORNISS. Daca produsul nu este certificat, este obligatoriu ca Ofertantul sa se oblige prin contract sa deruleze procedurile aferente certificarii, pana la testarea de acceptanta provizorie si sa puna la dispozitie documentatie, scheme, diagrame, sau orice alte documente necesare. Obligatiile de ordin financiar, tehnic si procedural aferente certificarii revin in exclusivitate Ofertantului si trebuie sa fie in conformitate cu legislatia aplicabila in Romania.
Ofertantul va asigura servicii de instruire „in regim train the trainers" pentru utilizarea si administrarea aplicatiei. Instruirea va fi realizata de instructor acreditat/certificat de producatorul aplicatiei.
Ofertantul va prezenta un angajament de la producatorul aplicatiei ca asigura suport tehnic on-site Beneficiarului pe toata perioada contractului, inclusiv in perioada de garantie.

6.9.2 Modul de validare a starii certificatelor

Pentru verificarea starii certificatelor emise va fi necesara implementarea unui serviciu de validare online a acestora, utilizand protocolul OCSP (Online Certificate Status Protocol) ce va fi conform cu standardul actual RFC 2560. Este obligatoriu ca serviciul de validare sa jurnalizeze toate evenimentele si actiunile ce au loc si sa le pastreze in siguranta pentru analiza si verificari ulterioare.
Serviciul de validare online a certificatelor digitale trebuie sa furnizeze un raspuns in timp real privind starea certificatelor iar accesul la certificatele si CRL-urilor autoritatilor se va realiza utilizand urmatoarele metode:
Preluarea dintr-un serviciu de directoare LDAP v3

Preluarea certificatelor si CRL-urilor prin intermediul protocolului HTTP (publicate pe un server web)

Preluarea certificatelor si CRL-urilor stocate local (hard disk)

De asemenea, solutia OCSP trebuie sa permita validarea certificatelor digitale si pe baza informatiilor extrase direct din baza de date a autoritatii de certificare.
In situatia in care serviciul primeste o cerere de validare a unui certificat pentru care nu are informatii atunci acesta trebuie sa se poata conecta la un alt serviciu OCSP care poate sa raspunda la aceasta cerere. Aceasta functionalitate trebuie sa capabila sa accepte rute configurabile pentru trimiterea cererilor. Astfel in functie de informatiile disponibile despre celelate servicii de OCSP si informatiile din certificatul ce se doreste validat cererea va fi trimisa direct catre serviciul care poate raspunde pentru starea respectivului certificat. De asemenea este necesar ca in cazul in care pentru un certificat acesta nu poate raspunde si nici nu are informatii despre serviciul care poate oferi validarea, prin configurare cererile sa fie trimise catre un serviciu OCSP implicit.
Serviciul va utiliza un dispozitiv criptografic certificat FIPS 140-2 level 3 (minim 500 de operatiuni RSA 1024/sec) pentru stocarea cheilor utilizate pentru semnarea raspunsurilor trimise catre client. Serviciul trebuie sa permita accesul la cheile private utilizate pentru semnarea raspunsului utilizand control dual, cu schema de tipul k din n. Astfel un numar minim de k operatori trebuie sa fie prezenti pentru pornirea serviciului si incarcarea cheilor private.
In vederea testarii diferitelor situatii de configurare este necesar ca solutia ce permite implementarea serviciului de OCSP sa poata fi configurata in mod software, fara utilizarea unui dispozitiv criptografic hardware pentru generarea si stocarea cheilor.
Pentru indeplinirea cerintelor de inalta disponibilitate solutia trebuie sa permita instalarea serviciului intr-o arhitectura ce suporta failover.
Interfata va fi si in limba romana. In acest sens se vor prezenta capturi de ecran ale aplicatiei si manuale de utilizare.
Ofertantul va prezenta angajamentul de la producatorul aplicatiei prin care acesta garanteaza ca asigura functionalitatile cerute prin caietul de sarcini.
Produsul ofertat trebuie sa fie existent si cu maturitate de cel putin 3 ani in piata.
Se va avea in vedere certificarea nationala ca produs de securitate la nivel minim **Secret de Serviciu** de catre ORNISS. Daca produsul nu este certificat, este obligatoriu ca Ofertantul sa se oblige prin contract sa deruleze procedurile aferente certificarii, pana la testarea de acceptanta provizorie si sa puna la dispozitie documentatie, scheme, diagrame sau orice alte documente necesare. Obligatiile de ordin financiar, tehnic si procedural aferente certificarii revin in exclusivitate Ofertantului si trebuie sa fie in conformitate cu legislatia aplicabila in Romania.
Ofertantul trebuie sa faca dovada ca are personal certificat de producatorul software-ului de validare pentru instalarea, configurarea si administrarea acestuia.
Ofertantul va prezenta un angajament de la producatorul aplicatiei ca va asigura la sediul producatorului aplicatiei servicii de instruire „in regim train the trainers" pentru utilizarea si administrarea aplicatiei.

Ofertantul va prezenta un angajament de la producatorul aplicatiei ca asigura suport tehnic on-site Beneficiarului pe toata perioada contractului, inclusiv in perioada de garantie.

6.9.3 Modul de marcare temporala

Cerintele de securitate ale beneficiarului impun cunoasterea cu exactitate a momentului semnarii unui anumit document. Pentru a indeplini aceste cerinte este necesara implementarea unui serviciu de marcare temporala accesibil de catre toti utilizatorii. Acest serviciu trebuie sa fie implementat cu respectarea standardului RFC 3161.
Serviciul va asigura nerepudierea actiunilor prin emiterea unor marci temporale semnate ce vor fi conforme cu RFC 3161 si vor contine cel putin urmatoarele:
Data si ora la care s-a realizat marcarea temporala

Semnatura electronica a serviciului de marcare pe amprenta electronica a documentului (digest-ul documentului)

Informatii prin care se poate identifica unic marca temporala in lista marcilor emise de serviciu; ofertantul va prezenta mecanismul utilizat prin care se garanteaza prevenirea emiterii de marci temporale din trecut

Serviciul va utiliza protocolul HTTP pentru comunicatia intre client (aplicatia sau sistemul care va crea marca temporala) si serviciul de marcare temporala. Pentru a respecta conditiile de acuratete impuse de un astfel de serviciu, este necesara sincronizarea cu sursa de timp a MSI, utilizand protocolul NTP.
Caracterul sensibil a acestui serviciu impune utilizarea unui dispozitiv criptografic certificat FIPS 140-2 level 3 (minim 500 de operatiuni RSA 1024/sec) pentru stocarea cheilor criptografice utilizate pentru semnarea marcilor temporale. Serviciul trebuie sa permita accesul la cheile private utilizate pentru semnarea token-ului de marcare temporala utilizand control dual, cu schema de tipul k din n. Astfel un numar minim de k operatori trebuie sa fie prezenti pentru pornirea serviciului si incarcarea cheilor private.
In vederea efectuarii unor operatiuni de testare, solutia trebuie sa permita instalarea si configurarea utilizand chei private stocate in containere software.
Pentru indeplinirea cerintelor de inalta disponibilitate solutia trebuie sa permita instalarea serviciului intr-o arhitectura ce suporta failover.
Interfata va fi si in limba romana. In acest sens se vor prezenta capturi de ecran ale aplicatiei si manuale de utilizare.
Ofertantul va prezenta angajamentul de la producatorul aplicatiei prin care acesta garanteaza ca asigura functionalitatile cerute prin caietul de sarcini.
Produsul ofertat trebuie sa fie existent si cu maturitate de cel putin 3 ani in piata.
Se va avea in vedere certificarea nationala ca produs de securitate la nivel minim **Secret de Serviciu** de catre ORNISS. Daca produsul nu este certificat, este obligatoriu ca Ofertantul sa se oblige prin contract sa deruleze procedurile aferente certificarii, pana la testarea de acceptanta provizorie si sa puna la dispozitie documentatie, scheme, diagrame sau orice alte documente necesare. Obligatiile de ordin financiar, tehnic si procedural aferente certificarii revin in exclusivitate Ofertantului si trebuie sa fie in conformitate cu legislatia aplicabila in Romania.
Ofertantul va asigura servicii de instruire „in regim train the trainers" pentru utilizarea si administrarea aplicatiei. Instruirea va fi realizata de instructor acreditat/certificat de producatorul aplicatiei.Ofertantul va prezenta un angajament de la producatorul aplicatiei ca asigura suport tehnic on-site Beneficiarului pe toata perioada contractului, inclusiv in perioada de garantie.

6.9.4 Modul de recuperare a cheilor private de criptare

Cerintele de securitate impun ca in cazul documentelor criptate sa existe o procedura prin care respectivele documente sa poata fi recuperate atunci cand dispozitivul criptografic nu mai exista sau nu mai poate fi utilizat (defect, pierdere, etc.). Pentru satisfacerera acestei conditii este necesar ca autoritatea de certificare sa implementeze un modul dedicat recuperarii cheilor private utilizate pentru criptare.
Cheile private de criptare trebuie pastrate in forma criptata utilizand chei de criptare diferite de cele de semnare ale autoritatilor de certificare.
Se va impune ca recuperarea acestor chei private sa necesite prezenta unui numar minim de operatori utilizand o schema prag de tip "K din N", unde din N administratori minim K trebuie sa fie prezenti pentru a putea efectua recuperarea cheilor.
Modulul de recuperare a cheilor private va utiliza un dispozitiv criptografic hardware certificat FIPS 140-2 level 3 (minim 500 operatiuni RSA 1024/sec).
Interfata va fi si in limba romana. In acest sens se vor prezenta capturi de ecran ale aplicatiei si manuale de utilizare.
Ofertantul va prezenta angajamentul de la producatorul aplicatiei prin care acesta garanteaza ca asigura functionalitatile cerute prin caietul de sarcini.

Se va avea in vedere certificarea nationala ca produs de securitate la nivel minim **Secret** de catre ORNISS. Daca produsul nu este certificat, este obligatoriu ca Ofertantul sa se oblige prin contract sa deruleze procedurile aferente certificarii, pana la testarea de acceptanta provizorie si sa puna la dispozitie documentatie, scheme, diagrame, cod sursa sau orice alte documente necesare. Obligatiile de ordin financiar, tehnic si procedural aferente certificarii revin in exclusivitate Ofertantului si trebuie sa fie in conformitate cu legislatia aplicabila in Romania.
Ofertantul va asigura servicii de instruire „in regim train the trainers" pentru utilizarea si administrarea aplicatiei. Instruirea va fi realizata de instructor acreditat/certificat de producatorul aplicatiei.Ofertantul va prezenta un angajament de la producatorul aplicatiei ca asigura suport tehnic on-site Beneficiarului pe toata perioada contractului, inclusiv in perioada de garantie.

6.9.5 Modulul de administrare a dispozitivelor criptografice ale utilizatorilor

Va oferi minim urmatoarele functionalitati:
administrarea dispozitivelor criptografice (schimbare pin, deblocare token, administrarea certificatelor de pe token)

posibilitate de administrarea a dispozitivelor criptografice de tip javacard (configurare appleti)

integrare cu modulul de recuperare a cheilor criptografice

Modulul va fi accesibil pe Web de catre utilizatori, prin protocol SSL cu dubla autentificare pentru realizarea operatiilor de administrare a dispozitivelor criptografice. Pentru cazurile in care dispozitivul criptografic nu mai este accesibil (PIN pierdut, dispozitiv pierdut sau distrus), modulul trebuie sa fie accesibil prin intermediul administratorilor care vor modifica corespunzator in sistem starea token-ului si de asemenea se va genera o cerere de revocare a certificatelor de pe acel token.
Modulul trebuie sa se poata integra cu Active Directory sau alte surse (de exemplu modul resurse umane) pentru preluarea automata a datelor noilor utilizatori carora li se vor distribui dispozitive criptografice si li se vor emite certificate digitale.
Interfata va fi si in limba romana.
Ofertantul va furniza, de la producator, pentru fiecare structura, cate o licenta pentru un numar nelimitat de smartcarduri sau token-uri USB si va prezenta angajamentul de la producator ca acesta va furniza aceste licente.
Ofertantul va prezenta angajamentul de la producatorul aplicatiei prin care acesta garanteaza ca asigura functionalitatile cerute prin caietul de sarcini.
Ofertantul trebuie sa faca dovada ca are personal certificat de producatorul software-ului pentru instalarea, configurarea si administrarea acestuia.

6.9.6 Specificatii tehnice

Formatul certificatelor digitale: ITU X.509 v3

Tipuri de certificate: admise conform RFC 5280, respectiv semnare, criptare, IPSEC, SSL/TLS, OCSP Signer, Timestamp Signer, S/MIME, semnare de cod, fara a se limita la cele aratate.

Algoritmi criptografici suportati:

Pentru semnatura : RSA

Pentru rezumat : SHA-1, SHA-2

Lungimea cheilor utilizatorilor: minim RSA 1024 biti

Lungimea cheilor autoritatilor: minim RSA 2048 biti

Biblioteci criptografice : conforme cu standardul FIPS 140-2 level 1

Standarde criptografice suportate: PKCS#1, PKCS#7, PKCS#10, PKCS#11, PKCS#12

Suport pentru configurarea politicilor de certificare

Suport pentru configurarea tipurilor de certificate

Publicarea certificatelor: server de tip LDAP v3

6.9.7 Migrarea infrastructurii PKI existente

Se va asigura continuitatea serviciilor asociate certificatelor digitale (emitere, revocare, distributie) prin migrarea datelor catre noua instanta fara intreruperea niciunuia dintre aceste servicii. Pentru a asigura continuitatea acestor servicii urmatoarele cerinte trebuiesc respectate:

- se va asigura utilizarea certificatele existente ale autoritatilor (ROOT si subordonate) in noua infrastructura. Aceasta cerinta include migrarea cheilor din cadrul echipamentelor hardware de tip HSM existente pe noile echipamente HSM; se va avea in vedere in principal aceasta cerinta la alegerea echipamentelor HSM pentru a furniza compatibilitatea cu vechile echipamente.

- se vor utiliza aceleasi politici si configuratii pentru emiterea certificatelor digitale. Valabilitatea certificatului, tipul cheii, extensiile specifice vor fi identice in noul sistem cu cele din vechiul sistem astfel inca in momentul in care un certificat va fi emis pe noua infrastructura nu se va putea face diferenta fata de vechiul certificat. Este permisa adaugarea de functionalitati care imbunatatesc ergonomia utilizarii certificatului (extensii suplimentare, informatii despre autoritate) sau securitate sporita (lungimi de chei mai mari) fara a elimina insa niciuna dintre functionalitatile existente.

- se vor utiliza aceleasi politici si configuratii pentru emiterea listelor de certificate revocate. Este critica functionarea fara intrerupere a serviciului de emitere a listelor de certificate revocate avand in vedere ca toata functionarea sistemului se bazeaza pe informatiile continute de acestea. Este necesara ca valabilitatea CRL-urilor sa ramana cea initiala si un CRL emis pe noua infrastructura sa fie identic cu un CRL emis pe vechea infrastructura. De asemenea este permisa adaugarea de functionalitati care sa imbunatateasca ergonomia utilizarii certificatelor digitale si a serviciilor de validare fara a elimina insa niciuna dintre functionalitatile existente.

- se va asigura serviciul de revocare a certificatelor pentru toate certificatele emise deja pe vechea infrastructura pana la expirarea acestora. Prin aceasta cerinta se impune ca toate certificatele valide, emise de catre vechea infrastructura, sa se regaseasca in cadrul noii instante pentru a putea fi manipulate conform ciclului de viata uzual al certificatelor (in principal este vorba de revocare). Nu este necesara importarea certificatelor expirate din vechea infrastructura, este recomandat a se evita aceasta decizie datorita volumului mare de date si a lipsei de utilitate a unei asemenea masuri. Daca insa in cadrul procesului tehnologic nu este posibila aceasta separare se vor avea in vedere toate optimizarile sistemului pentru a acomoda atat certificatele existente cat si pe cele ce urmeaza a fi emise.

- toate datele despre utilizatorii sistemului, existente in cadrul vechiului sistem, se vor regasi in noul sistem. Este obligatoriu sa nu trebuiasca furnizate informatiile de identificare inca odata pentru acestia. De asemenea este obligatoriu ca toate componentele care folosesc la comunicatiile intre sistemul CA si sistemele conectate/dependente sa functioneze fara a fi necesare modificari la nivelul acestora.

6.10 Platforma validarea documentelor semnate electronic și a mărcii temporale

Aplicaţia pentru validarea documentelor semnate electronice şi a mărcii temporale trebuie să aibă implementate următoarele funcţionalităţi:

Să permită monitorizarea automată a unuia sau mai multor cont-uri de e-mail în vederea identificării mesajelor care au ataşamente semnate electronic și marcate temporal;

Să valideze în mod automat ataşamentele semnate electronic și marcate temporal atât din punct de vedere al integrităţii acestora cât şi din punct de vedere al validităţii certificatelor digitale cu care a fost realizată semnătura electronică și marca temporală;

Să valideze în mod automat documente semnate electronic și marcate temporal, aflate în diferite directoare care pot fi configurate din aplicație;

Să salveze în mod automat fişierele valide semnate electronic și marcate termporal, în clar, într-un director (directoare) configurabil(e). Directorul trebuie să poată fi configurat de către administratorul aplicaţiei;

Să permită integrarea în mai multe fluxuri de validare, fie prin monitorizarea mai multor directoare și salvarea fișierelor validate în directoare parametrizabile în funcție de sursa monitorizată, fie prin rularea unei instanțe pentru fiecare flux de validare;

Să ridice alerta în cazul în care nu se poate efectua validarea documentelor; administratorul să poată configura trimiterea de mesaje automate de avertizare către operatorii sistemului și către emitenții documentelor;

Să permită validarea certificatelor digitale cu care s-a realizat semnarea digitală și marcarea temporală prin toate cele trei opţiuni enumerate mai jos:

Off-line – presupune ca toate certificatele din lanţul de certificare precum şi listele de certificate revocate să fi

fost preinstalate;

LDAP – prin căutarea automată pe un director LDAP a lanţului de certificare precum şi a listelor de certificate

revocate; aplicaţia trebuie să permită atât configurarea adresei de căutare în directorul LDAP cât şi utilizarea

adresei de căutare menţionate în certificatul digital;

Utilizând un server OCSP – aplicaţia trebuie să permită configurarea adresei de conectare la server-ul OCSP.

Să logheze toate acţiunile efectuate şi să permită obţinerea de rapoarte referitor la acestea;

În cazul fişierelor semnate multiplu în sensul standardului RFC 5652, aplicaţia va trebui să valideze fiecare certificat în parte;

Să suporte sistemele de operare Windows.

Pentru indeplinirea cerintelor de inalta disponibilitate solutia trebuie sa permita instalarea serviciului intr-o arhitectura ce suporta failover.
Interfata va fi si in limba romana. In acest sens se vor prezenta capturi de ecran ale aplicatiei si manuale de utilizare.

6.11 Platforma pentru semnarea automatizată a documentelor electronice

Aplicaţia pentru semnarea automatizată a documentelor electronice trebuie să aibă implementate următoarele funcţionalităţi:
Fişierele procesate să aibă o noua extensie (*.p7s) și pictograma fişierului să fie modificată;

Noile fişiere semnate să poată fi procesate utilizând orice altă aplicaţie compatibilă cu standardul PKCS#7;

Semnarea se va realiza în mod automat pe baza unui token criptografic care conține certificatul de semnare;

Să poată semna documentele identificate într-un anumit director;

Fişierele care au fost semnate se vor muta într-un alt director şi se şterg din directorul curent;

Să fie compatibilă cu dispozitive de tip HSM (Hardware Secure Module) pentru semnarea unui volum mare de documente;

Să permită operatorului întreruperea procesului de semnare și reluarea acestuia de la momentul opririi;

Aplicaţia trebuie să fie capabilă să transmită fişierele semnate către anumite adrese de e-mail configurabile de administratorul aplicaţiei;

Toate acţiunile aplicaţiei vor fi logate în mod amănunţit în fişier dedicat, care va avea o structură ce va permite exportul facil al acestor loguri în fişiere de tip tabelar, sau într-o bază de date.

Aplicația trebuie să poată semna și marca temporal cel puțin 80 de documente/secundă.

Pentru indeplinirea cerintelor de inalta disponibilitate solutia trebuie sa permita instalarea serviciului intr-o arhitectura ce suporta failover.
Interfata va fi si in limba romana. In acest sens se vor prezenta capturi de ecran ale aplicatiei si manuale de utilizare.

7. SERVICII DE IMPLEMENTARE PROIECT

7.1 Servicii amenajare DataCenter

Implementarea centrului de date se va face intrun spatiu dedicat pus la dispozitie de beneficiar in locatia de implementare a proiectului. In acest sens, in urma ofertei tehnice, in faza de analiza se va elibera un document de proiectare din care sa rezulte configuratia finala a spatiului amenajat, echipamente folosite, modul de amplasare, interconectarea loc, trasee de cablu, scheme electrice de conectare.
In acest sens, vor avea loc urmatoarele activitati:

- Evaluarea arhitecturii generale a incintei care va gazdui DataCenter-ul;
- Evaluarea caracteristicilor de instalare si pozitionare a instalatiei de aer conditionat;
- Evaluarea caracteristicilor de legare si extindere a sistemului de alimentare cu energie electrica;
- Evaluarea caracteristicilor pentru sistemul de securitate fizica;
- Evaluarea caracteristicilor pentru sistemul de cablare structurata.

In urma elaborarii documentului de proiectare si agreearea acestuia de catre beneficiar se vor executa lucrarile de amenajare in conformitate cu propunerea tehnica din oferta tehnica. Ofertantul va trebui sa puna la dispozitie personal calificat si autorizat sa execute toate lucrarile aferente fiecarei faze si componente din documentul de proiectare. Ofertantul va asigura tot personalul necesar, logistica si materialele pentru executarea lucrarilor de amenajare a spatiului DataCenter si va avea obligatia sa execute toate lucrarile de amenajare, livrare si instalare de echipamente si materiale ce reies din oferta tehnica si documentul de proiectare.

7.2 Servicii de livrare, instalare si configurare a echipamentelor hardware

Dupa incheierea lucrarilor de amenajare DataCenter, ofertantul va trebui sa execute serviciile de livrare, instalare si configurare a echipamentelor harwdare.
Primul pas este realizarea unui proiect tehnic de catre ofertant din care sa reiasa echipamentele si componentele software implicate in proiect cu cantitatile de rigoare, toate activitatile de instalare si configurare a echipamentelor, a solutiilor software de baza, a planului de adresare, a interconectarii cu alte sisteme, jurnal de cabluri si arhitectura generala a sistemului cu fluxuri operationale.
Urmatoarea faza este intocmirea unui grafic de livrari cu beneficiarul si agreearea acestuia de ambele parti, cu respectarea termenelor si conditiilor si oferta tehnica si contract. Acesta faza este urmata de livrarea efectiva a echipamentelor si acceptanta cantitativa a lor de catre beneficiar. Livrarea se va face la locatia de proiect a beneficiarului. Ofertantul va asigura tot personalul necesar, logistica si materialele pentru livrarea echipamentelor conform cu oferta tehnica si proiectul tehnic.
Dupa acceptarea cantitativa a echipamentelor hardware, in baza proiectului tehnic ofertantul va presta serviciile de instalare si configurare. Ofertantul va trebui sa puna la dispozitie personal calificat cu o inalta pregatire profesionala pentru a executa toate serviciile aferente fiecarei faze de instalare si configurare a echipamentelor hardware si va avea obligatia sa execute toate serviciile de instalare si configurare ce reies din oferta tehnica si proiectul tehnic.

7.3 Servicii de livrare, instalare si configurare software de baza

Livrarea software de baza se va realiza odata cu echipamentele hardware, pe baza graficelor de livrare intocmite in aceea faza. Livrarea se va realiza la locatia de proiect a beneficirului.
Dupa incheierea serviciilor de instalare si configurare a echipamentelor hardware, ofertantul va realiza instalarea si configurarea software de baza. Parametrii tehnici ce trebuie respectati si implemnetati in aceasta faza se regasesc in proiectul tehnic: distributia resurselor, dimensionarea mediilor si a masinilor, componentele software ce se instaleaza in fiecare masina, interconectarea, setarile de retea, etc.
Ofertantul va trebui sa puna la dispozitie personal calificat cu o inalta pregatire profesionala pentru a executa toate serviciile aferente fiecarei faze de instalare si configurare a software de baza si va avea obligatia sa execute toate serviciile de instalare si configurare ce reies din oferta tehnica si proiectul tehnic.

7.4 Servicii de dezvoltare

Serviciile de dezvoltare a functionalitatilor aplicatiei vor include:

- Dezvoltarea componentelor software cu respectarea specificatiilor caietului de sarcini;
- Integrarea componentelor software in cadrul sistemului si interconectarea cu sistemele aferente;
- Testarea functionalitatilor solutiei software dezvoltate din care sa reiasa indeplinirea cerintelor;

- Configurarea pentru intrarea in productie a sistemului software dezvoltat;
- Acceptanta finala a beneficiarului pe solutia software dezvoltata.

Ofertantii trebuie sa prezinte metodologia care sta la baza procesului de dezvoltare, configurare si testare interna, si vor prezenta corespondenta cu procedurile de analiza si proiectare.
Solutia dezvoltata si implementata la nivelul sistemul SICAP va fi de tip web based si nu va avea restrictii de utilizatori. Solutia propusa trebuie sa fie baza pe servicii web iar arhitectura propusa trebuie sa respecte principiile unei arhitecturi SOA. Ofertantii trebuie sa prezinte si sa faca dovada ca procedurile de implementare din cadrul propriei organizatii se integreaza cu procedurile de dezvoltare, configurare si testare interna.

7.5 Servicii de testare functionala si de performanta

Pentru a face dovada ca sistemul propus si implementat este unul de inalta performanta in conformitate cu specificatiile caietului de sarcini, ofertantul declarant castigator va realiza servicii de testare functionala si de performanta a sistemului inainte de a intra in productie. In cadrul ofertei tehnice, ofertantii vor atasa un livrabil in care sa prezinte sumar testele propuse si uneltele de testare in conformitate cu solutia si arhitectura propusa.
In cadrul activitatilor de testare, ofertantul va trebui sa asigure minim urmatoarele servicii si livrabile:

Livrabilele Serviciilor de testare:		**Cerinte minime obligatorii**
Strategia si planificarea testarii	Metodologie si/sau Strategie de testare	Se va creea o strategie de testare conform standardelor ISO29119 urmand metodologiile ISEB si ISTQB, aceasta urmand sa contina scopul si obiectivele testarii, criteriile de intrare si iesire, mediul de testare, modalitatea de executie a testelor, tipurile de teste, management-ul defectelor, management-ul release-urilor, niveluri de testare, roluri si responsabilitati. Se va propune un flux de lucru optimizat pentru procesul de testare care sa se integreze cu fluxurile de lucru propuse de celelelte echipe din cadrul proiectului;
	Fluxuri de lucru si proceduri automatizate	Sa se creeze un set de proceduri de lucru pentru testeri care sa descrie actiunile de urmat in anumite situatii intalnite in cadrul procesului de testare; Sa automatizeze in platforma propusa fluxurile de lucru si procedurile din strategia de testare
	Planurile de testare	Se va documenta modul cum ofertantul abordeaza testarea sistemului, obiectul efortului de testare, activitatile necesare pregatirii si efectuarii nivelurilor de testare, mediile de testare, livrabilele, rolurile si responsabilitatile pentru testare, procedurile de testare si metoda de raportare. Planul de testare va fi creeat pentru 70 cazuri de testare automate de functionalitate si 20 cazuri de testare de performanta. Planul de testare trebuie sa includa minim trei scenarii de testare de performanta si minim 10 scenarii de testare de functionalitate. Continut minim: obiectele supuse testarii obiectivele si perimetrul testelor cerintele mediului de testare functiile de testat si rezultatele asteptate abordarea de testare si tipurile de teste prevazute abordarea folosita in crearea/gestionarea datelor de test succesiunea testelor din matricea testelor, cu dependentele corespunzatoare modelate in instrumentele de testare responsabilitatile in procesul de testare riscurile si actiunile de preintampinare a defectelor, cu determinarea impactului, probabilitatii si responsabilului cu preintampinarea lor criterii de intrare/iesire, care sa asigure ca sunt pregatite conditiile de incepere a testelor planificate, respectiv finalizarea testelor planificate si eliminarea defectelor livrabilele implicate

		• criterii de acceptanta.
Documentarea testarii	Specificatii detaliate de testare	Trebuie sa contina cel putin: • cazurile de test • descrierea datelor de test, cu referire la datele de intrare si la baza de date peste care se executa testele • scenariile de test (lanturi de executie a cazurilor de test, pentru a simula procese end-to-end) • matricea cerintelor functionale/non-functionale, matricea testelor de acoperire a cerintelor (mapeaza cazurile de test cu cerintele) • matricea conditiilor de test, matricea testelor de acoperire a conditiilor de test (mapeaza cazurile de test cu conditiile de test)
Executia testarii	Testarea Functionala Automata	• Se va permite testarea automata si creearea de teste functionale manuale si a celor de regresie. Va trebui sa se capteze, sa se verifice si sa se redea interactiunile utilizatorului in mod automat, astfel incat testerii sa identifice si sa raporteze rapid efectele aplicatiei. • Solutia trebuie sa permita lucrul colaborativ al testerilor. • Solutia trebuie sa permita automatizarea testelor functionale si a celor de regresie. Solutia trebuie sa fie usor de folosit, permitand crearea de teste sofisticate cu cat mai putine cunostinte. Acest lucru trebuie sa fie posibil prin captarea activitatilor procesului desfasurat direct din ecranul aplicatiei si generarea automata a testelor. Solutia trebuie sa ajute utilizatorul sa identifice mai usor defectele si activitati duplicate, sa genereze documentatia si sa semnaleze defectele dezvoltatorilor. • Solutia trebuie sa permita in mod usor expertilor sa adauge, modifice, ruleze si sa elimine pasi de testare. • Solutia trebuie sa se poata actualiza automat cand se recompileaza o aplicatie iar actualizarea trebuie sa fie propagata pentru toate testele care se leaga de o anumita componenta. • Solutia trebuie sa permita testarea functionala atat manuala, cat si automata, creearea testelor, mentenanta si executia lor cat si managementul datelor de test. Solutia trebuie sa permita reducerea timpului necesar ciclurilor de test prin implicarea in procesul de creeare a testelor si optimizare a procesului de calitate a expertilor in procesele de afaceri, prin automatizarea creerii de planuri de testare si eficientizarea mentenantei testelor atunci cand se modifica aplicatiile. • Solutia propusa trebuie sa permita executia de teste functionale manuale si automate. • Solutia trebuie sa permita colaborarea usoara intre grupuri de lucru prin administrarea si partajarea definitiilor si obiectelor aplicatiei. • Trebuie sa se poata combina testarea functionala manuala cu cea automata pentru ca expertii care cunosc detalii despre dezvoltarea si testarea aplicatiei sa poata participa la procesul de optimizare a calitatii. • Trebuie sa se permita generarea de teste automate intr-un mod flexibil, prin combinarea automatizarii testelor cu documentatia, astfel permitand masurarea calitatii din definitii abstracte. Utilizatorul trebuie sa poata defini teste manuale sau automate care sa faca diferite activitati pentru fiecare componenta si trebuie sa poata converti acele componente in componente automate, asociindu-le cu anumite zone ale aplicatiei. • Solutia trebuie sa permita administrarea centralizata a cazurilor de

		test, a testelor si a planului de testare. - Solutia trebuie sa permita asamblarea proceselor de business care urmeaza a fi testate folosind componente reutilizabile. Ea trebuie sa permita acest lucru prin drag-and-drop de componente in script, dintr-o lista arborescenta. - Solutia propusa trebuie sa includa un minim de 70 script-uri automate de testare creeate pe aplicatia indicata de Beneficiar - Solutia trebuie sa fie capabla sa genereze in mod automat documentatia in timp ce echipa de testare creeaza testele. - Documentatia trebuie sa poata fi exportata in formate compatibile cu procesoarele de text, pentru a fi personalizabila. - Solutia trebuie sa permita testarea functionala atat manuala, cat si automata, creearea testelor, mentenanta si executia lor cat si managementul datelor de test. Solutia trebuie sa permita reducerea timpului necesar ciclurilor de test prin implicarea in procesul de creeare a testelor si optimizare a procesului de calitate a expertilor in procesele de afaceri, prin automatizarea creerii de planuri de testare si eficientizarea mentenantei testelor atunci cand se modifica aplicatiile. - Solutia trebuie sa ofere automat si in timp real functionalitati de control al acoperirii cu teste a specificatiilor functionale si de agregare a rezultatelor testelor la nivel de specificatie functionala - Solutia trebuie sa afiseze automat si in timp real rezultatele testarii la nivelul fiecarei actiuni din fluxul de lucru indiferent de granularitatea acestuia si de cate specificatii functionale compun acea activitate - Solutia trebuie sa poata optimiza testarea manuala astfel incat timpul petrecut de tester cu citirea si manipularea cazurilor de testare manuale sa fie minim - Solutia trebuie sa fie optimizata pentru a fi folosita de utilizatori fara cunostinte tehnice de testare automata sau manuala - solutia trebuie sa permita resurselor non-it rularea de teste automate si manuale fara sa necesite cunostinte tehnice. - Solutia trebuie sa permita executia de teste functionale manuale si automate. - Solutia trebuie sa permita administrarea centralizata a cazurilor de test, a testelor si a planului de testare. - Solutia trebuie sa permita creearea de teste automate si utilizatorilor (testeri) care nu au notiuni de scripting sau programare. - Soluția permite administrarea și editarea mai multor teste și librării concomitent , reducând timpul petrecut de testeri la depanarea scripturilor și facilitând astfel procesul de testare. - Soluția permite, în cazul unui test format din mai multe operații, rularea oricărei dintre operații fără a fi necesară rularea întregului test, reducând considerabil timpul de testare. - Solutia permite compararea directă a fișierelor PDF și rularea Checkpointurilor (verificarilor) pe acestea
	Testarea de performanta	- Asigurarea functionarii la un nivel ridicat de calitate al sistemului propus impune functionarea corecta in conditii de incarcare maxima fara erori semnificative. Pentru aceasta, va trebui utilizata o solutie de testare de performanta care sa asigure verificarea corecta a capacitatii sistemului si robustetea acestuia. Platforma de testare de performanta ce urmeaza a fi utilizata va avea urmatoarele caracteristici:

		- trebuie sa permita validarea performantei aplicatiilor ce se vor implementa. Solutia trebuie sa poata genera probleme de performanta si sa diagnosticheze provenienta acestora premergator punerii in productie a sistemului. - trebuie sa poata prezice comportamentul sistemului si performantele aplicatiilor prin verificarea daca noile dezvoltari sau actualizari intrunesc cerintele de performanta definite, permitand identificarea si eliminarea problemelor de performanta pe durata etapei de dezvoltare a sistemului. - trebuie sa permita reducerea timpului necesar procesului de creare a scripturilor prin inregistrarea scripturilor la nivel de interfata cu utilizatorul, prin click-uri pe ecran, astfel incat scripturile sa poata fi generate automat - vor trebui furnizate minim 20 script-uri de testare de performanta si sa se ruleze minim 3 teste de performanta (3 iteratii) pe o aplicatie indicata de catre Beneficiar - Solutia trebuie sa fie capabila sa genereze in mod virtual un numar minim de 500 de utilizatori concurenti, pentru a simula activitati reale, folosind resurse hardware minimale. - Solutia trebuie sa fie capabila sa determine dimensionarea optima a platformelor hardware si software in functie de pasii proceselor business. - Solutia trebuie sa permita cresterea incarcarii virtuale pentru a permite simularea incarcarii de varf pentru procesele business selectate pentru testare. - Solutia trebuie sa masoare rezultatele performantei simulate cu indicatorii de performanta ai procesului si sa recomande modificarile necesare a fi efectuate asupra aplicatiei software testate. - Solutia trebuie sa permita re-rularea testelor folosind mediul de lucru modificat pentru a valida eficacitatea modificarilor. - Solutia trebuie sa contina module avansate de analiza si diagnosticare. - Solutia trebuie sa permita simularea de scenarii business folosite in mediul real si sa fie compatibila cu cele mai noi standarde si metodologii de testare. - Solutia trebuie sa poate izola problemele legate de performanţa şi sa reduca timpul mediu până la soluţionarea blocajelor de performanţa ale aplicaţiei testate. - Solutia trebuie sa poata verifica daca noile dezvoltari sau actualizari indeplinesc criteriile specifice de performanta pre-definite. - Solutia trebuie semnaleze cu usurinta blocajele la nivel de utilizatori finali, sistem si cod - Solutia trebuie sa includa un motor pentru scanarea datelor despre utilizatorul final, sistem şi diagnostice şi sa ofere cele mai probabile 10 cauze ale încetinirii sistemului. - trebuie sa testeze anduranţa sistemului pe intreaga arhitectura a acestuia, aplicând fluxuri consistente, măsurabile şi repetabile si sa utilizeze datele pentru a identifica problemele de scalabilitate ce pot afecta utilizatorii reali în producţie. - trebuie sa capteze timpii de răspuns ai utilizatorului final pentru procesele de afaceri şi tranzacţiile cheie, pentru a determina dacă beneficiarul poate îndeplini condiţiile acordurilor asumate privind nivelul calităţii serviciilor oferite.

		- trebuie sa contina un modul distinct dedicate analizei rezultatelor care poate fi folosit pe alte statii de lucru (in afara de platforma de testare) pentru o interpretare si analiza ulterioara a rezultatelor. - trebuie sa permita dezvoltarea de script-uri intr-un modul care poate fi folosit separat de server-ul de testare de performanta pentru a facilita dezvoltarea sau mentenanta de script-uri in parallel cu testele de performanta - trebuie sa permita dezvoltarea usoara a script-urilor preferabil prin tehnologii de tip click&script - trebuie sa permita maximum de flexibilitate in conceperea script-urilor pentru a le putea adapta celor mai complexe procese de business - trebuie sa permita creearea de script-uri cu minimum de cunostinte de scripting sau programare - Solutia trebuie sa contina functionalitati predefinite care sa ii permita creearea de component/actiuni distincte care la randul lor sa se poata recombine in orice ordine in acelasi script pentru a simula procese complexe cu elemente aleatorii - trebuie sa permita simularea de procese care sa contina activitati repetate de un numar variabil si aleator de ori in cadrul aceluiasi script - trebuie sa contina un numar suficient de monitoare care sa analizeze toate componentele sistemului - trebuie sa agrege toate rezultatele furnizate de monitoare, sa le trimita catre un instrument de analiza in care sa poata fi suprapuse si editate diferite grafice - Instrumentul sau modulul de analiza a rezultatelor de performanta trebuie sa contina functionalitati de tip drill down pentru a analiza in detaliu rezultatele - Instrumentul sau modulul de analiza trebuie sa permita efectuarea de insemnari direct pe graficele analizate - Instrumentul sau modulul de analiza trebuie sa permita exportul rezultatelor prin template-uri de rapoarte in formate uzuale cum ar fi docx, html sau pdf - trebuie sa se poata izola problemele de performanta ale aplicatiilor implementate si sa reduca MTTR al acestora. Solutia trebuie sa asigure informatii privind actiunile posibile pentru a rezolva problemele de performanta. - trebuie sa contina elemente neintruzive de monitorizare a performanţei care sa obţina şi sa afişeaze în timp real datele despre performanţă la fiecare nivel, server şi componentă a sistemului si sonde de diagnosticare care adună date la nivel de cod pentru a izola blocajele de la nivel de declaraţie sau metodă SQL. - trebuie sa poate trece prin tranzacţiile lente ale utilizatorului final ajungând la componenta, metoda sau instrucţiunea SQL blocată, ajutând la rezolvarea problemelor de memorie, excepţii şi alte probleme similar - trebuie sa detecteze în mod automat care componente sunt „active” atunci când este efectuată o anumită tranzacţie şi sa colecteze date cu privire la acestea pentru analiză. - trebuie sa fie capabila sa sa verifice trei cele mai defavorabile scenarii din activitatile de business actuale
	Testarea de acceptanta	- Va fi executata de catre Beneficiar cu assitenta prestatorului. - Va fi testare functionala avand ca scop validarea produsului livrat

		🕐 Ofertantul va oferi instruire verificatorilor numiti de beneficiar pentru a folosi platforma de testare

8. RESURSE

8.1 Instruire

În programul de instruire trebuie evidenţiate următoarele aspecte:
Categoria de utilizatori din cadrul fiecărei faze de instruire.

Perioada fiecărei faze de instruire (numărul de zile).

Cunoştinţe suplimentare pentru fiecare faza de instruire. (daca este cazul)

Cunoştinţe minime pentru fiecare faza de instruire.

Cunoştinţe suplimentare pentru fiecare categorie de utilizatori (daca este cazul).

Asigurarea suportului de curs in limba romana pentru utilizatori

Va avea loc o instruire a specialiştilor care vor opera sistemul din partea AADR si a celor ce vor realiza instruirea utilizatorilor finali (pentru modul de folosire a aplicaţiei, a specialiştilor în informatică (pentru detalii tehnice privind depanarea si administrarea sistemului), precum şi a conducerii (în privinţa posibilităţilor oferite de sistem). Se va furniza suport de training pentru personalul de specialitate. Se va specifica numărul de ore pentru instruirea personalului, pe categorii de personal.
Documentaţie minimala ce trebuie livrata împreuna cu aplicaţia:
Help contextual

Manualul de operare.

Planul de instruire al utilizatorilor va cuprinde :
Aria de funcţionalitate din cadrul sistemului cuprinsă în cadrul fiecărei faze de instruire;

Categoria de utilizatori din cadrul fiecărei faze de instruire;

Perioada fiecărei faze de instruire (numărul de zile);

Cunoştinţe suplimentare pentru fiecare fază de instruire;

Cunoştinţe minime pentru fiecare fază de instruire;

Cunoştinţe suplimentare pentru fiecare categorie de utilizatori;

Asigurarea suportului de curs în limba romană pentru utilizatorii sistemului;

Suport de training pentru personalul de specialitate.

Se vor utiliza cele mai moderne metode de învăţământ : expunerea, prelegerea, dialogul interactiv, exemplificarea practică, jocul de rol.
Conţinutul curriculei va fi structurat pe competenţe. Se vor adapta tipurile de activităţi de învăţare la specificul curriculei. Activităţile didactice vor fi structurate pe unităţi de învăţare.
Cursurile de instruire pentru modulele aplicative ale SICAP vor fi disponibile de asemenea in cadrul platformei colaborative de instruire.

8.2 Resurse material

Resursele materiale implicate în realizarea proiectului sunt cele existente în sediul Centrul National de Management pentru Societataea Informationala din Strada Italiana nr. 22, sector 2, cod 020976, Bucuresti

Echipamentele ce urmează a fi achiziționate in cadrul proiectului vor fi livrate în prima perioada de implementare a proiectului, astfel încât vor putea fi folosite in faza de implementare propriu-zisă a proiectului.
Pe durata perioadei de școlarizare vor exista o serie de resurse materiale ce vor fi utilizate. Acestea vor fi asigurate de beneficiar:
Sala pentru desfășurarea cursurilor (în locațiile în care se implementează proiectul);

Camera serverelor în centrul de date;

Conexiune internet pentru portalul public;

Conexiune rețea pentru toate locațiile.

9. GARANTIE SI SUPORT

9.1 Garantie

Beneficiarul investiției, AADR, este entitatea care va asigura operarea și mentenanța investiției pentru o perioadă de cel puțin 5 ani după implementarea proiectului.
AADR, în calitate de structură de specialitate, cu personalitate juridică, va prevedea în procesul de fundamentare al bugetului anual sumele necesare asigurării operării și întreținerii (inclusiv service-ul și mentenanța) investiției la parametri optimi de funcționare.
Activitățile preconizate a se implementa în cadrul proiectului fac parte dintr-un plan de acțiune mai larg derulat de către instituția beneficiară care vizează asigurarea unei mai bune funcționări a instituției prin automatizarea activității interne. Acest fapt va asigura continuarea și extinderea lor dincolo de perioada de implementare a proiectului.
În condițiile în care se anticipează un ritm de dezvoltare susținut, instituția beneficiară dispune de resursele financiare, tehnice și umane necesare pentru continuarea și extinderea activităților începute în cadrul prezentului proiect.
În analiza sustenabilității financiare a proiectului s-au avut în vedere următoarele elemente revizionare:
decalajul orizontului de timp: nu va exista la nivel național o evoluție nefavorabilă și/sau întârzieri ale componentelor programului care să influențeze derularea proiectului;

beneficiarul va avea resurse suficiente pentru acoperirea cheltuielilor pe perioada de implementare, în limita angajamentului;

cheltuielile cu personalul și cele cu materialele nu au impact asupra costurilor proiectului (nu este necesară suplimentarea resurselor);

nu vor exista elemente neprevăzute care să inducă o creștere a costurilor și/sau amânare a proiectului, fie în faza de implementare, fie în cea de operare.

Analizând indicatorii de profitabilitate financiari, putem concluziona ca proiectul nu se poate susține singur din punct de vedere financiar si necesita sprijin financiar. Indicatorii financiarii sunt negativi deoarece proiectul de investiții este negenerator de profit, beneficiile aduse de prezentul proiect fiind de natura sociala. Indicatorii de rentabilitate economica analizați (RIRE si VNAE) demonstrează ca proiectul este oportun din punct de vedere economico-social (aduce beneficii economico-sociale) si instituția are nevoie de proiect prin beneficiile aduse în economie (proiectul merită intervenție financiara din partea POS CCE). Din punct de vedere al sustenabilității financiare, proiectul generează un flux de numerar cumulat pozitiv in fiecare an al perioadei de previziune, astfel putem aprecia că proiectul propus spre finanțare prezintă o stabilitate ridicata din punctul de vedere al rentabilității financiare, dat fiind că și analiza de senzitivitate si de risc nu a identificat nici o variabila critica cu impact semnificativ.
În concluzie, întrucât costurile de realizare a investiției sunt acoperite complet din resursele bugetului instituției plus fonduri nerambursabile, pe întreaga perioadă de analiză, fluxul financiar este zero. Aceasta demonstrează sustenabilitatea financiară a proiectului.
Resursele financiare necesare mentenanței investiției urmează să fie alocate din bugetul AADR. Activitățile propuse în vederea continuării proiectului și care ar urma să fie finanțate din aceste resurse în perioada post-implementare sunt:

- AADR se va angaja ca prin contractul/contractele încheiate pe perioada implementării cu diverși furnizori să asigure obligatoriu garanția și mentenanța aplicației. De asemenea, beneficiarul se va angaja

să asigure mentenanța aplicației și funcționarea permanentă a acesteia în perioada de post implementare, respectiv 5 ani după finalizarea implementării proiectului, cu excepția perioadelor de mentenanță planificate. Mai mult, AADR va depune copia contractului pentru mentenanța proiectului, odată cu ultima cerere de rambursare.

- Contractul/contractele încheiate de beneficiar cu diverși furnizori pentru garanția și mentenanța aplicației, vor asigura obligativitatea funcționării permanente a acesteia în perioada de post-implementare. Acest lucru va fi prevăzut în caietul de sarcini întocmit pentru organizarea procedurii pentru achiziția sistemului informatic integrat.
- Realizarea în perioada de mentenanță de actualizări periodice care vor consta în adăugarea de module noi în funcție de necesitățile utilizatorilor;
- Extinderea aplicației în perioada de mentenanță care va presupune asigurarea, în cadrul portalului dedicat acesteia, a unor servicii online în funcție de necesitățile identificate în rândul utilizatorilor, astfel încât mediul online să devină mai cuprinzător;
- Reorganizarea activității în perioada de mentenanță cu ajutorul noilor tehnologii prin integrarea de noi instrumente informatice care să acopere și alte segmente din activitatea instituției.

În privința resurselor umane calificate, solicitantul își consolidează portofoliul de competențe în cadrul proiectului, creând un nucleu de specialiști care să reprezinte o resursă pe termen lung care va asigura o capacitate solida din punct de vedere numeric și al expertizei tehnice în vederea menținerii rezultatului proiectului pentru o perioada de minimum 5 ani după implementarea proiectului. Proiectul prevede inclusiv activitate de instruire pentru personalul tehnic și astfel, cunoștințele și abilitățile dobândite sau dezvoltate le vor permite să valorifice la maxim oportunitățile pe care le poate oferi sistemul ce va fi implementat. Pe de altă parte, echipa formată în cadrul proiectului va disemina aceste cunoștințe, instruind resursele umane care ar putea fi atrase ca urmare a unei viitoare extinderi a activităților demarate în cadrul proiectului.

9.2 Servicii de support hardware

Serviciile de garanție pentru toate echipamentele furnizate vor fi asigurate de către furnizorul sistemului pentru o perioadă de 3 ani de la data livrării acestora.

9.3 Servicii de support software

Serviciile de suport software vor fi asigurate de către furnizorul sistemului pentru o perioadă de 1 an de la data punerii in funcțiune a produselor software.
În timpul perioadei de suport, Furnizorul va asigura serviciile de suport pentru:

- Customizarile și parametrizare / extensiile din cadrul implementării proiectului;
- Produsele / componentele utilizate în dezvoltarea sistemului informatic;
- Platforma hardware / sistem de operare utilizat în baza Service Level Agreement (SLA).

9.4 Descrierea nivelului de support

In cadrul SLA-ului furnizorul va acorda următoarele servicii de suport:

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

Pentru a permite o identificare proactivă a unor posibile soluții, se va asigura acces la o baza de cunoștințe tehnice și/sau documentație tehnică specificate prin intermediul centrului de Help Desk.
În acest sens, va fi desemnat un singur punct de intrare pentru toate incidentele legate de soluția informatică furnizata și anume către Administratorul de Servicii al Furnizorului.
Administratorul de Servicii al Furnizorului va:

- administra și monitoriza incidentele;

- lua legătură cu persoana desemnată ca punct de contact din partea beneficiarului, pentru analiza stărilor incidentelor deschise;

- va răspunde tuturor intrebărilor legate de incidente.

Problemele ridicate de beneficiar vor fi înregistrate de către specialişti ai Furnizorului, în cadrul unei aplicaţii de tip HELPDESK. Serviciul HELPDESK trebuie sa aiba un minim de 10 operatori active operationali pentru preluarea incidentelor.
Suportul va fi furnizat intre [09:00 şi 18:00] ora României, de Luni pana Vineri cu excepţia sărbătorilor legale.
Se va asigura diagnosticarea unui incident pentru determinarea problemei de baza.
Se va monitoriza în permanenta incidentul pana la închiderea acestuia.
Beneficiarul va avea acces la aplicaţia de tip HELPDESK pentru a monitoriza incidentele.

Urmărirea incidentelor:

Persoana desemnată ca punct de contact din partea beneficiarului va lansa un incident, Administratorul de Servicii al Furnizorului primind o notificare pe e-mail sau fax. Fiecare incident va avea ataşat un nivel de prioritate (ca în exemplele de mai jos) care să reflecte impactul problemei asupra funcţionarii sistemului. Initial ataşarea nivelului de prioritate se va face cu ajutorul Administratorului de Servicii al Furnizorului pentru a facilita rezolvarea incidentului în timp util.
Nivelul de prioritate poate fi modificat cu acordul părţilor în funcţie de evoluţia incidentului.
Furnizorul poate sa îşi rezerve dreptul de a modifica un nivelul de prioritate a incidentului, dar cu anunţarea în avans a echipei beneficiarului
Serviciile de Suport vor fi furnizate sub incidenţa Clauzelor de Confidenţialitate.

Nivele de Prioritate;

Definiţiile nivelelor de prioritate sunt cele de mai jos:

Nivel Prioritate	**Descriere**
Urgent	**Impact Major** asupra funcţionarii sistemului din nodul central Problema împiedica desfasurarea activităţii institutiei, procesul de activitate este serios afectat şi nu mai poate continua pierderea funcţionalitatilor devenind critice.
Critic	**Impact Semnificativ** asupra funcţionarii sistemului din nodul central Problema impiedica desfasurarea în condiţii normale a activităţii utilizatorilor. Nici o soluţie alternativa nu este disponibila, iar activitatea utilizatorilor poate totuşi continua, insa intr-un mod restrictiv.
Major	**Impact Mediu** asupra funcţionarii sistemului Problema afecteaza minor funcţionalitatile sistemului. Impactul reprezintă un inconvenient care necesita soluţii alternative pentru refacerea funcţionalitatilor.
Minor	**Impact Minim** asupra funcţionarii sistemului Problema nu afecteaza funcţionalitatile sistemului. Rezultatul este o eroare minora care nu impiedica desfasurarea în bune condiţii a activităţii utilizatorilor.

Asistenţă este de tipul:
• on site (numai la sediul central al beneficiarului)
în cazul incidentelor cu nivel de prioritate "urgent" asistenţă va fi asigurata 24x7, fiind disponibila pana cand problema va fi rezolvata. Pentru aceasta beneficiarul va furniza o persoana de contact, disponibila 24x7, care să furnizeze informaţii, să testeze soluţii şi să aplice soluţiile ftirniżate.

Timpi de răspuns şi rezoluţii

Furnizorul va respecta următorii timpi de răspuns, dar în corelaţie cu nivelul de prioritate:

Nivel prioritate	Timp de răspuns	Timp soluţie provizorie temporara	Timp de remediere
Urgent	4 ore	1 zi	1 zi
Critic	4 ore	1 zi	1 zi
Major	4 ore	2 zile	3 zile

Minor	4 ore	2 zile	5 zile

Timpii de mai sus sunt calculaţi din momentul în care Furnizorul a fost instiintat de apariţia problemelor.
La sfarsitul fiecărui caz deschis Furnizorul va efectua o analiza a cauzelor care au dus la producerea deranjamentului şi va fi inclusa în recomandarea finala.
Furnizorul va garanta ca SLA-ul mai sus mentionat se bazeaza pe servicii de suport pentru soluţia software furnizata în cadrul acestui contract. în cazul în care apare un deranjament hardware, timpii de răspuns vor fi calculaţi, de asemenea, pe baza tabelului de mai sus.
Definiţiile, descrise mai jos se vor aplica la Service Level Agreement:

- **Timp de Răspuns:** Timpul scurs de la contactul iniţial dintre beneficiar şi HELPDESK şi răspunsul primit de la echipa de suport tehnic a Furnizorului către beneficiar. Aceasta acţiune se va desfasura prin intermediul telefonului.

- **Timp de Remediere:** Durata de timp până la oferirea soluţiei finale

- **Remediere Temporara:** O modificare în cadrul procedurilor sau datelor care să evite erorile fara folosirea defectuoasa a produselor.

- **SLA:** Service Level Agreement identifică funcţionalitatile şi defineşte procesele care implica livrarea de către Furnizor a diferite servicii de suport către Beneficiar.

- **Suport:** Telefonul de suport tehnic, asistenţă web şi e-mail oferite de Furnizor pentru a ajuta Beneficiarul în rezolvarea problemelor aparute; Suportul este oferit la un Major

- Release al produsului şi la un Release Secvenţial Anterior al produsului. Furnizorul va oferi de asemenea asistenţă tehnica pentru versiunile mai vechi ale produsului, dar rezolvarea problemei ar putea fi limitata la instalarea unui Major Release.

- **HELPDESK:** Un centru de asistenţă tehnica ce oferă serviciul de preluare a cererilor prin telefon, web şi e-mail operat de către personalul care face parte din suportul Furnizorului oferind asistenţă pentru componenentele soluţiei informatice integrate furnizate.

Ofertantul va detalia in oferta tehnica modul in care va asigura mentenanta hardware, mentenanta software, si modul de soluţionare a incidentelor

10. LIVRABILELE PROIECTULUI

Furnizorul va asigura livrarea tuturor elementelor necesare si incluse in oferta sa pentru a asigura satisfacerea cerinţelor enuntate in caietul de sarcini. Furnizorul poarta intreaga responsabilitatea pentru costuri de import, asigurare, manipulare, transport si instalare fizica in locaţia Beneficiarului.
In cadrul fazelor de derulare a proiectului, oferantul declarat castigator va prezenta urmatoarele livrabile de proiect:
Specificatii tehnice functionale

Document proiectare amenajare DataCenter

Proiect tehnic

Plan de testare software

Plan de testare de securitate

Descrierea testelor software

Descrierea testelor de securitare

Raport de testare software

Raport de testare de securitate

Plan de instruire

Suport de curs

Manuale de utilizare

Manuale de administrare.

Ofertantul va prezenta planificarea activităţilor propuse, în interdependenţa acestora - un grafic Gantt. Acesta va respecta toate cerinţele explicite din cadrul caietului de sarcini.
Planul trebuie să menţioneze care sunt termenele cheie (milestones) pe care ofertantul si-a propus sa le respecte pentru atingerea obiectivelor.
Ofertantul trebuie să menţioneze expres în plan acele termene care sunt obligatorii aşa cum reiese din Caietul de sarcini. Nerespectarea acestora este eliminatorie.
Ofertantul va detalia care sunt resursele (experţii cheie si non cheie numiţi generic prin competentele lor) pe care le va aloca pentru fiecare etapă şi activitate a proiectului.
Graficul de proiect nu va cuprinde activităţi cu o durată individuală mai mare de 1 săptămână (7 zile calendaristice) pentru prima etapă a proiectului (etapa de analiză/iniţializare) şi de 2 săptămâni (14 zile calendaristice) pentru restul etapelor proiectului, pentru demonstrarea înţelegerii complete şi concrete a complexităţii proiectului şi a activităţilor concrete pe care ofertantul le va avea de derulat. În cazul in care graficul de implementare prezentat nu va respecta acest criteriu de calitate, oferta tehnica va fi respinsa. Nu se vor pune întrebări de clarificare pentru detalierea planului de implementare pe durata evaluării ofertelor.
Ofertantul va prezenta o descriere detaliată a abordării pentru implementarea proiectului, prin detalierea fiecăreia dintre activităţile incluse în graficul Gantt pe care îl va prezenta. Pentru fiecare activitate se vor prezenta durata, experţii implicaţi, efortul estimat din partea resurselor (măsurat în zile-om la 8 ore/zi) rezultatul aşteptat şi eventualele dependenţe de activităţi/resurse ale beneficiarului. Se vor identifica livrabilele principale ale serviciilor de implementare prestate, precum şi acceptanţele parţiale.

11. PREZENTARE OFERTA TEHNICA

Oferta tehnica trebuie sa adreseze punctual toate cerintele din Documentatia de Atribuire; pentru fiecare cerinta se va detalia modalitatea de indeplinire. Ofertele care vor mentiona doar conformitate cu cerinta si nu va detalia pentru fiecare cerinta modalitate de realizare vor fi considerate ca neconform. In cazul in care cerintele nu sunt indeplinite in totalitate cerintele din cadrul Documentatiei de Atribuire, ofertele vor fi considerate neconforme.
Modul de organizare al ofertei tehnice trebuie sa faciliteze urmarirea indeplinirii cerintelor si sa includa fara a se limita, urmatoarele:
Arhitectura tehnica detaliata a soluţiei ofertate

Descrierea tehnica a componentelor solutiei ofertate

Documentatia tehnica a produselor incluse in cadrul ofertei

Maparea clara intre arhitectura propusa, componentele solutiei propuse si componentele cerute in cadrul documentatiei de atribuire

Matricea de conformitate cu toate cerintele proiectului; se va include documentatie care sa faca dovada conformitatii cu cerintele tehnic (documentatie tehnica producatori, brosuri produse, etc.). Oferta tehnica va include toate documentele necesare pentru a dovedi caracteristicile fiecărui componente ofertata (producător, produs, documentatie tehnica de specialitate) si va include si codurile unice de identificare de la producător care identifica produsele oferite.

Plan de testare de securitate (descrierea sumara a tipurior de teste de securitate a sistemului)

Plan de testare functionala si de performanta (descriere sumara a tipurilor de teste si uneltele folosite pentru testare)

Planul de management al proiectului

Graficul de derulare a contractului cu includerea tuturor activitatilor

Modalitatea de asigurare a serviciilor (metodologie dezvoltare, proceduri de suport tehnic, metodologie de testare, metodologie testare de securitate etc.)

In cazul unei asocieri, se va mentiona in oferta tehnica rolul si responsabilitatile fiecarui membru al asocierii in dereularea proiectului.

Ofertantul trebuie sa prezinte o propunere de plan detaliat de migrare a datelor. Planul trebuie sa prezinte toate etapele necesare preluarii datelor din SEAP in noul sistem.

Ofertantul trebuie sa prezinte o propunere de plan de tranzitie pentru perioada intrarii in productie a sistemului dezvoltat in cadrul proiectului. Planul de tranzitie trebuie sa tina cont de faptul ca derularea achizitiilor publice nu trebuie sa fie impactata de trecerea la noul sistem.

In cadrul fazelor de derulare a proiectului, oferantul declarat castigator va prezenta urmatoarele livrabile de proiect: Specificatii tehnice functionale, Document proiectare amenajare DataCenter, Proiect tehnic, Plan de testare software, Descrierea testelor software, Raport de testare software, Plan de instruire, Suport de curs, Manuale de utilizare, Manuale de administrare.

Manager de proiect – Mirela TOMA
Asistent coordonator – Roxana POPESCU
Membru proiect – Simona BAJENARU
Responsabil implementare IT – Gabriel – Catalin DUMITRU
Responsabil financiar – Alexandra COSTACHE